Panduan Developer

AWS Config

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

AWS Config: Panduan Developer

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

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Apa itu AWS Config? ... 1
Pertimbangan ... 1
Cara Menggunakan AWS Config ... 1
Administrasi Sumber Daya ... 2
Audit dan Kepatuhan ... 2
Mengelola dan Memecahkan Masalah Perubahan Konfigurasi ... 2
Analisis Keamanan ... 2
Solusi Mitra ... 3
Fitur ... 3
Cara AWS Config Kerja ... 4
Penemuan Sumber Daya ... 5
Pelacakan Sumber Daya ... 5
Pengiriman Item Konfigurasi ... 6
Kontrol Akses ke AWS Config ... 9
Terminologi dan konsep ... 10
AWS Config Antarmuka ... 11
Manajemen Sumber Daya ... 11
Pencatat Konfigurasi ... 12
Saluran Pengiriman ... 6
AWS Config Aturan ... 14
Paket Kesesuaian ... 17
Agregator ... 18
AWS Integrasi Layanan ... 19
AWS Organizations ... 19
AWS Control Tower ... 19
AWS CloudTrail ... 20
AWS Security Hub ... 20
AWS Trusted Advisor ... 20
AWS Audit Manager ... 21
AWS Systems Manager ... 21
AWS Firewall Manager ... 22
Host EC2 Khusus Amazon ... 22
Application Load Balancer ... 22
AWS CodeBuild ... 23

AWS X-Ray ... 23
AWS Service Management Connector ... 23
Amazon API Gateway ... 23
Support Wilayah ... 24
Pertimbangan ... 24
Daftar Wilayah yang Didukung ... 25
Service Limits ... 29
Informasi Tambahan ... 31
AWS Kit Pengembangan Perangkat Lunak untuk AWS Config ... 32
Memulai ... 34
Mendaftar untuk AWS ... 34
Mendaftar untuk Akun AWS ... 34
Buat pengguna dengan akses administratif ... 35
Cara Memulai dengan AWS Config ... 36
Menyiapkan (Konsol) ... 36
Pengaturan ... 36
Pengaturan 1-klik ... 37
Pengaturan manual ... 40
Menyiapkan (AWS CLI) ... 47
Pengaturan ... 48
Prasyarat ... 48
Memulai AWS Config ... 114
Memverifikasi pengaturan ... 117
Bekerja dengan AWS SDKs ... 119
Pencatat Konfigurasi ... 121
Pertimbangan untuk perekam konfigurasi terkelola pelanggan ... 121
Pertimbangan untuk perekam konfigurasi terkait layanan ... 123
Layanan yang didukung ... 123
Deteksi drift untuk perekam konfigurasi ... 125
Memulai perekam konfigurasi terkelola pelanggan ... 125
Menghentikan perekam konfigurasi terkelola pelanggan ... 126
Mengubah frekuensi perekaman untuk perekam konfigurasi terkelola pelanggan ... 126
Mengganti nama perekam konfigurasi terkelola pelanggan ... 129
Melihat perekam konfigurasi Anda ... 130
Menghapus perekam konfigurasi Anda ... 132
Saluran Pengiriman ... 133

Pertimbangan ... 133
Terminologi ... 134
Komponen Item Konfigurasi ... 135
Melihat Saluran Pengiriman ... 137
Memperbarui Saluran Pengiriman ... 138
Mengganti nama Saluran Pengiriman ... 143
Mengirimkan Snapshot Konfigurasi ... 144
Mengirimkan Snapshot Konfigurasi ... 144
Memverifikasi Status Pengiriman ... 145
Melihat Snapshot Konfigurasi ... 146
Melihat Snapshot Konfigurasi ... 146
Contoh Snapshot Konfigurasi ... 147
Contoh Pemberitahuan ... 152
Contoh Pemberitahuan Perubahan Item Konfigurasi ... 153
Contoh Pemberitahuan Pengiriman Riwayat Konfigurasi ... 168
Contoh Konfigurasi Pengiriman Snapshot Mulai Pemberitahuan ... 169
Contoh Konfigurasi Pemberitahuan Pengiriman Snapshot ... 170
Contoh Pemberitahuan Perubahan Kepatuhan ... 171
Contoh Aturan Evaluasi Mulai Pemberitahuan ... 174
Contoh Pemberitahuan Perubahan Item Konfigurasi Besar ... 175
Contoh Pemberitahuan Gagal Pengiriman ... 178
AWS Config Dasbor ... 180
Kepatuhan dan Inventarisasi Sumber Daya ... 180
AWS Config Metrik Penggunaan dan Sukses ... 182
Manajemen Sumber Daya ... 185
Jenis Sumber Daya yang Didukung ... 186
Amazon AppStream ... 187
Amazon AppFlow ... 188
... 188
Amazon API Gateway ... 188
Amazon Athena ... 189
Amazon Bedrock ... 190
Amazon CloudFront ... 190
Amazon CloudWatch ... 191
Amazon CodeGuru ... 191
Amazon Cognito ... 192

Amazon Connect 193
Amazon Detective 194
Amazon DynamoDB 194
Amazon EC2 194
Amazon ECR 203
Amazon ECS 204
Amazon EFS 205
Amazon EKS 205
Amazon EMR 206
Amazon EventBridge 206
Amazon Forecast 207
Amazon Fraud Detector 207
Amazon GuardDuty 208
Amazon Inspector 209
Amazon IVS 209
Amazon Keyspaces 210
OpenSearch Layanan Amazon 210
Amazon Personalize 211
Amazon Pinpoint 212
Amazon QLDB 213
Amazon Kendra 213
Amazon Kinesis 213
Amazon Lex 214
Amazon Lightsail 214
Amazon Lookout for Metrics 215
Amazon Lookout for Vision 215
Amazon Macie 216
Amazon Managed Grafana 216
Layanan Terkelola Amazon untuk Prometheus 216
Amazon MemoryDB 216
Amazon MQ 217
Amazon MSK 217
Amazon QuickSight 218
Amazon Redshift 218
Amazon RDS 220
Amazon Route 53 221

Amazon SageMaker AI 223
Amazon SES 224
Amazon SNS 225
Amazon SQS 225
Amazon S3 225
Amazon WorkSpaces 227
AWS Amplify 228
AWS AppConfig 228
AWS App Runner 229
AWS App Mesh 230
AWS AppSync 231
AWS Audit Manager 231
AWS Auto Scaling 231
AWS Backup 232
AWS Batch 233
AWS Manajemen Penagihan dan Biaya 234
AWS Budgets 234
AWS Certificate Manager 234
AWS CloudFormation 235
AWS CloudTrail 235
AWS Cloud9 235
AWS Cloud Map 236
AWS CodeArtifact 237
AWS CodeBuild 237
AWS CodeDeploy 237
AWS CodePipeline 238
AWS Config 239
AWS DMS 240
AWS DataSync 240
AWS Device Farm 242
AWS Elastic Beanstalk 242
Resolusi Entitas AWS 243
AWS FIS 244
AWS Global Accelerator 244
AWS Glue 244
AWS Ground Station 245

AWS HealthLake ... 246
AWS IAM ... 246
AWS IoT ... 247
AWS KMS ... 251
AWS Lambda ... 252
AWS Mainframe Modernization ... 252
AWS Network Firewall ... 252
AWS Network Manager ... 253
AWS Panorama ... 255
AWS Private CA ... 255
AWS Resilience Hub ... 256
Penjelajah Sumber Daya AWS ... 256
AWS RoboMaker ... 256
AWS Signer ... 257
AWS Secrets Manager ... 257
AWS Security Hub ... 258
AWS Service Catalog ... 258
AWS Shield ... 259
AWS Step Functions ... 259
AWS Systems Manager ... 260
AWS Transfer Family ... 260
AWS WAF ... 261
AWS X-Ray ... 263
Penyeimbang Beban Elastis ... 263
MediaConnect ... 265
MediaPackage ... 265
MediaTailor ... 266
Cakupan Sumber Daya berdasarkan Ketersediaan Wilayah ... 266
Amerika Utara dan Selatan ... 266
Eropa ... 308
Asia Pasifik ... 345
Tiongkok ... 390
Afrika dan Timur Tengah ... 412
GovCloud ... 438
AWS Sumber Daya Rekaman ... 462
Pertimbangan ... 462

Sumber Daya Regional dan Global ... 463
AWS Config Aturan dan jenis sumber daya global ... 467
Frekuensi perekaman ... 468
Sumber daya yang tidak direkam ... 469
Sumber daya perekaman (Konsol) ... 470
Sumber daya perekaman (AWS CLI) ... 474
Tidak termasuk sumber daya ... 482
Menghentikan perekaman ... 483
Merekam Sumber Daya Pihak Ketiga (AWS CLI) ... 483
Menambahkan Sumber Daya ... 484
Merekam Item Konfigurasi ... 487
Membaca Item Konfigurasi ... 488
Menghapus Sumber Daya ... 489
Konfigurasi Perangkat Lunak Perekaman ... 490
Prasyarat ... 490
Konfigurasi Perangkat Lunak Perekaman ... 491
Mencari Sumber Daya ... 493
Melihat Sumber Daya ... 494
Melihat kepatuhan (Konsol) ... 495
Melihat kepatuhan (AWS SDKs) ... 495
Melihat Riwayat Kepatuhan ... 503
Melihat Riwayat Kepatuhan (Konsol) ... 504
Melihat Riwayat Kepatuhan (AWS CLI) ... 504
Untuk Sumber Daya dan Aturan ... 510
Meminta Riwayat Kepatuhan ... 511
Menandai Sumber Daya Anda ... 512
Pembatasan Terkait Penandaan ... 513
Mengelola Tag dengan Tindakan AWS Config API ... 513
AWS Aturan Config ... 515
Pertimbangan ... 515
Support Wilayah ... 518
Komponen Aturan ... 526
Bagaimana AWS Config Aturan Bekerja ... 526
Jenis Pemicu ... 527
Mode Evaluasi ... 528
Metadata Aturan ... 530

Aturan Terkelola 531
Daftar Aturan Terkelola 532
Daftar Aturan Terkelola berdasarkan Mode Evaluasi 1012
Daftar Aturan Terkelola berdasarkan Jenis Pemicu 1036
Daftar Aturan Terkelola berdasarkan Ketersediaan Wilayah 1059
Membuat Aturan Terkelola Dengan AWS CloudFormation Template 1635
Aturan Kustom 1636
Aturan Kebijakan Kustom 1637
Aturan Lambda Kustom 1637
Perbedaan format untuk Aturan AWS Config Kustom 1637
Membuat Aturan Kebijakan Kustom 1638
Membuat Aturan Lambda Kustom 1644
Mengelola Sumber Daya yang Dihapus untuk Aturan Lambda Kustom 1667
Aturan Terkait Layanan 1668
Aturan Organisasi 1669
Pertimbangan 1670
Deployment 1671
Support Wilayah 1671
Menambahkan Aturan 1675
Menggunakan konsol 1675
Menggunakan AWS SDKs 1678
Memperbarui Aturan 1682
Menggunakan konsol 1682
Menggunakan AWS SDKs 1683
Menghapus Aturan 1686
Pertimbangan 1687
Menggunakan konsol 1687
Menggunakan AWS SDKs 1688
Aturan Melihat 1690
Menggunakan konsol 1690
Menggunakan AWS SDKs 1691
Mengaktifkan Evaluasi Proaktif 1702
Menggunakan konsol 1703
Menggunakan AWS SDKs 1705
Mengirim Evaluasi ke Security Hub 1709
Kirim Evaluasi Aturan ke Security Hub 1710

Mengevaluasi Sumber Daya dengan Aturan ... 1710
Menghapus Hasil Evaluasi ... 1714
Pemecahan Masalah ... 1715
Paket Kesesuaian ... 1718
Dasbor Paket Kesesuaian ... 1719
Menavigasi Halaman Utama Paket Kesesuaian ... 1719
Prasyarat ... 1720
Langkah 1: Mulai AWS Config Merekam ... 1720
Langkah 2: Prasyarat Tambahan berdasarkan Jenis Paket Kesesuaian ... 1720
Support Wilayah ... 1726
Pemeriksaan Proses ... 1733
Contoh Template ... 1734
Membuat Cek Proses ... 1734
Mengubah Status Kepatuhan ... 1735
Lihat dan Edit ... 1736
Templat Contoh Paket Kesesuaian ... 1737
AWS Paket Kesesuaian Pagar Pembatas Detektif Menara Kontrol ... 1741
Praktik Terbaik Operasional untuk Beban Kerja Material ABS CCIG 2.0 ... 1741
Praktik Terbaik Operasional untuk Beban Kerja Standar ABS CCIG 2.0 ... 1976
Praktik Terbaik Operasional untuk ACSC Essential 8 ... 2150
Praktik Terbaik Operasional untuk ACSC ISM ... 2178
Praktik Terbaik Operasional untuk AI dan ML ... 2319
Praktik Terbaik Operasional untuk Amazon API Gateway ... 2320
Praktik Terbaik Operasional untuk Amazon CloudWatch ... 2320
Praktik Terbaik Operasional untuk Amazon DynamoDB ... 2320
Praktik Terbaik Operasional untuk Amazon S3 ... 2320
Praktik Terbaik Operasional untuk APRA CPG 234 ... 2320
Praktik Terbaik Operasional untuk Manajemen Aset ... 2558
Praktik Terbaik Operasional untuk AWS Backup ... 2558
Praktik Terbaik Operasional untuk Manajemen AWS Identitas Dan Akses ... 2558
Praktik Terbaik Operasional untuk Pilar Keandalan AWS Kerangka Well-Architected ... 2559
Praktik Terbaik Operasional untuk Pilar Keamanan AWS Kerangka Well-Architected ... 2626
Praktik Terbaik Operasional untuk BCP dan DR ... 2791
Praktik Terbaik Operasional untuk BNM T RMi ... 2792
Praktik Terbaik Operasional untuk Profil Kontrol Cloud Sedang Pusat Keamanan Siber Kanada (CCCS) ... 3125

Praktik Terbaik Operasional untuk Tolok Ukur AWS Yayasan CIS v1.4 Level 1 4703
Praktik Terbaik Operasional untuk Tolok Ukur AWS Yayasan CIS v1.4 Level 2 4741
Praktik Terbaik Operasional untuk Kontrol Keamanan Kritis CIS v8 IG1 4789
Praktik Terbaik Operasional untuk Kontrol Keamanan Kritis CIS v8 IG2 4892
Praktik Terbaik Operasional untuk Kontrol Keamanan Kritis CIS v8 IG3 5067
Praktik Terbaik Operasional untuk CIS Top 20 5258
Praktik Terbaik Operasional untuk CISA Cyber Essentials 5341
Praktik Terbaik Operasional untuk Layanan Informasi Peradilan Pidana (CJIS) 5551
Praktik Terbaik Operasional untuk CMMC 2.0 Level 1 5689
Praktik Terbaik Operasional untuk CMMC 2.0 Level 2 5810
Praktik Terbaik Operasional untuk Layanan Komputasi 6222
Praktik Terbaik Operasional untuk Ketahanan Data 6223
Praktik Terbaik Operasional untuk Layanan Database 6223
Praktik Terbaik Operasional untuk Data Lakes dan Layanan Analytics 6223
Praktik Terbaik Operasional untuk DevOps 6223
Praktik Terbaik Operasional untuk EC2 6224
Praktik Terbaik Operasional untuk Enkripsi dan Manajemen Kunci 6224
Praktik Terbaik Operasional untuk Panduan Keamanan Siber ENISA untuk SMEs 6224
Praktik Terbaik Operasional untuk Esquema Nacional de Seguridad (ENS) Rendah 6401
Praktik Terbaik Operasional untuk Medium Esquema Nacional de Seguridad (ENS) 6512
Praktik Terbaik Operasional untuk Esquema Nacional de Seguridad (ENS) High 6639
Praktik Terbaik Operasional untuk FDA Judul 21 CFR Bagian 11 6774
Praktik Terbaik Operasional untuk FedRAMP (Rendah) 7153
Praktik Terbaik Operasional untuk FedRAMP (Sedang) 7434
Praktik Terbaik Operasional untuk FedRAMP (Bagian Tinggi 1) 8026
Praktik Terbaik Operasional untuk FedRAMP (Bagian Tinggi 2) 8657
Praktik Terbaik Operasional untuk FFIEC 8792
Praktik Terbaik Operasional untuk Katalog Kriteria Kepatuhan Komputasi Awan Jerman (C5) 9030
Praktik Terbaik Operasional untuk Gramm Leach Bliley Act (GLBA) 9119
Praktik Terbaik Operasional untuk GxP EU Annex 11 9177
Praktik Terbaik Operasional untuk Keamanan HIPAA 9349
Praktik Terbaik Operasional untuk IRS 1075 9875
Praktik Terbaik Operasional untuk K-ISMS 10101
Praktik Terbaik Operasional untuk Load Balancing 10193
Praktik Terbaik Operasional untuk Penebangan 10194

Praktik Terbaik Operasional untuk Layanan Manajemen dan Tata Kelola 10194
Praktik Terbaik Operasional untuk Pemberitahuan MAS 655 10194
Praktik Terbaik Operasional untuk MAS TRMG 10237
Praktik Terbaik Operasional untuk Pemantauan 10470
Praktik Terbaik Operasional untuk NBC TRMG 10471
Praktik Terbaik Operasional untuk NERC CIP BCSI 10949
Praktik Terbaik Operasional untuk Prinsip Keamanan Cloud NCSC 11021
Praktik Terbaik Operasional untuk Kerangka Penilaian Cyber NCSC 11134
Praktik Terbaik Operasional untuk Jaringan dan Layanan Pengiriman Konten 11331
Praktik Terbaik Operasional untuk NIST 800-53 rev 4 11331
Praktik Terbaik Operasional untuk NIST 800-53 rev 5 11672
Praktik Terbaik Operasional untuk NIST 800 171 12354
Praktik Terbaik Operasional untuk NIST 800 172 12707
Praktik Terbaik Operasional untuk NIST 800 181 12781
Praktik Terbaik Operasional untuk NIST 1800 25 13317
Praktik Terbaik Operasional untuk NIST CSF 13483
Praktik Terbaik Operasional untuk Kerangka Privasi NIST v1.0 13867
Praktik Terbaik Operasional untuk NYDFS 23 14123
Praktik Terbaik Operasional untuk NZISM 3.8 14324
Praktik Terbaik Operasional untuk PCI DSS 3.2.1 14474
Praktik Terbaik Operasional untuk PCI DSS 4.0 (Tidak termasuk jenis sumber daya global) 14822
Praktik Terbaik Operasional untuk PCI DSS 4.0 (Termasuk jenis sumber daya global) 15139
Praktik Terbaik Operasional untuk Sumber Daya yang Dapat Diakses Publik 15530
Praktik Terbaik Operasional untuk Kerangka Keamanan Cyber RBI untuk UCBs 15531
Praktik Terbaik Operasional untuk RBI MD-ITF 15580
Praktik Terbaik Operasional untuk Layanan Keamanan, Identitas, dan Kepatuhan 15743
Praktik Terbaik Operasional untuk Tanpa Server 15743
Praktik Terbaik Operasional untuk Layanan Penyimpanan 15743
Praktik Terbaik Operasional untuk SWIFT CSP 15744
Praktik Terbaik Keamanan untuk Amazon Elastic Container Service (Amazon ECS) 15779
Praktik Terbaik Keamanan untuk Amazon Elastic File System (Amazon EFS) 15780
Praktik Terbaik Keamanan untuk Amazon Elastic Kubernetes Service (Amazon EKS) 15780
Praktik Terbaik Keamanan untuk Amazon CloudFront 15780
Praktik Terbaik Keamanan untuk OpenSearch Layanan Amazon 15780
Praktik Terbaik Keamanan untuk Amazon Redshift 15781

Praktik Terbaik Keamanan untuk Amazon Relational Database Service (Amazon RDS) .. 15781
Praktik Terbaik Keamanan untuk AWS Auto Scaling 15781
Praktik Terbaik Keamanan untuk AWS CloudTrail 15781
Praktik Terbaik Keamanan untuk AWS CodeBuild 15782
Praktik Terbaik Keamanan untuk Amazon ECR 15782
Praktik Terbaik Keamanan untuk AWS Lambda 15782
Praktik Terbaik Keamanan untuk AWS Network Firewall 15782
Praktik Terbaik Keamanan untuk Amazon SageMaker AI 15783
Praktik Terbaik Keamanan untuk AWS Secrets Manager 15783
Praktik Terbaik Keamanan untuk AWS WAF 15783
Contoh Template dengan Tindakan Remediasi 15783
Membuat Template Kustom 15784
Terminologi 15784
Menyesuaikan template 15784
Menyebarkan Paket Kesesuaian 15789
Mengedit Paket Kesesuaian 15792
Menghapus Paket Kesesuaian 15793
Pertimbangan 15794
Untuk menghapus paket kesesuaian 15794
Melihat Paket Kesesuaian 15795
Melihat Riwayat Kepatuhan 15798
Melihat Timeline Kepatuhan 15799
Meminta Riwayat Kepatuhan 15800
Mengelola Paket Kesesuaian Organisasi 15801
Pertimbangan 15802
Deployment 15803
Support Wilayah 15804
Pemecahan Masalah 15807
Status gagal untuk paket kesesuaian 15807
Aturan menggantung dalam paket kesesuaian 15809
Remediasi 15811
Support Wilayah 15811
Menyiapkan Remediasi Manual 15815
Menyiapkan Remediasi Otomatis 15817
Menghapus Tindakan Remediasi 15819
Agregator 15821

Kasus penggunaan 15821
Terminologi 15822
Support Wilayah 15822
Dasbor Agregator 15827
Menggunakan Dasbor Aggregator 15827
Dasbor Kepatuhan 15830
Dasbor Inventaris 15832
Membuat Agregator 15834
Mendaftarkan Administrator yang Delegasi 15840
Mengedit Agregator 15842
Menghapus Agregator 15844
Mengotorisasi Akun Agregator 15844
Pertimbangan 15845
Menambahkan Otorisasi 15845
Menghapus Otorisasi 15847
Pertimbangan 15847
Menghapus Otorisasi 15847
Melihat Agregator 15848
Pemecahan Masalah 15849
Pertanyaan Lanjutan 15852
Fitur 15853
Komponen Kueri 15853
Sinopsis 15853
Parameter 15854
Contoh 15854
Editor Kueri (Konsol) 15855
Pertimbangan 15855
Gunakan AWS Contoh Query 15855
Buat kueri kustom Anda 15856
Editor Kueri (AWS CLI) 15857
Pertimbangan 15857
Data Konfigurasi Sumber Daya Kueri 15858
Menyimpan Kueri 15860
Lihat semua Kueri Tersimpan 15860
Dapatkan Detail Kueri Tersimpan 15861
Hapus Kueri Tersimpan 15861

Prosesor kueri bahasa alami 15862
Pertimbangan 15862
Kueri menggunakan prosesor kueri bahasa alami 15855
Contoh petunjuk 15863
Memberikan umpan balik 15867
Support Wilayah 15867
Contoh Pertanyaan 15868
Contoh Pertanyaan Hubungan 15874
Batasan 15876
Kisaran CIDR notation/IP 15877
Beberapa properti dalam array 15878
Support Wilayah 15879
Menghapus Data 15884
Mengatur Periode Retensi Data (Konsol) 15886
Keamanan 15888
Perlindungan Data 15889
Enkripsi Data dalam Transit 15890
Enkripsi Data dalam Transit 15890
Identity and Access Management 15890
Audiens 15891
Mengautentikasi dengan identitas 15891
Mengelola akses menggunakan kebijakan 15895
Bagaimana AWS Config bekerja dengan IAM 15898
Contoh kebijakan berbasis identitas 15905
AWS kebijakan terkelola 15924
Izin untuk Peran IAM 16094
Memperbarui Peran IAM 16098
Izin untuk Bucket Amazon S3 16100
Izin untuk Kunci KMS 16104
Izin untuk Topik Amazon SNS 16107
Pemecahan Masalah 16111
Menggunakan Peran Terkait Layanan 16113
Tanggapan Insiden 16115
Validasi Kepatuhan 16115
Ketahanan 16117
Keamanan Infrastruktur 16117

Analisis Konfigurasi dan Kelemahan 16117
Pencegahan "confused deputy" lintas layanan 16118
Praktik Terbaik 16118
Pembuatan Log dan Pemantauan 16120
Pencatatan log 16120
AWS Config Informasi di CloudTrail 16120
Memahami Entri File AWS Config Log 16121
Contoh File Log 16122
Pemantauan 16129
Menggunakan Amazon SQS 16130
Menggunakan Amazon EventBridge 16132
Titik akhir Amazon VPC 16139
Buat Endpoint VPC 16139
FAQs 16140
Tidak dapat melihat perubahan konfigurasi terbaru saya 16140
Dapatkah saya berharap untuk melihat perubahan konfigurasi saya segera? 16140
Hubungan Tidak Langsung di AWS Config 16140
Apa itu hubungan sumber daya? 16140
Apa hubungan langsung dan tidak langsung sehubungan dengan sumber daya? 16141
Hubungan tidak langsung mana yang AWS Config mendukung? 16141
Skenario mana yang menggunakan hubungan tidak langsung? 16143
Bagaimana item konfigurasi dibuat karena hubungan langsung dan tidak langsung? 16145
Apa item konfigurasi yang dihasilkan karena hubungan tidak langsung? 16145
Bagaimana cara menonaktifkan hubungan tidak langsung? 16147
Bagaimana cara mengambil data konfigurasi yang terkait dengan hubungan tidak langsung? 16147
Contoh kode 16148
Hal-hal mendasar 16148
Tindakan 16149
Riwayat Dokumen 16185
Pembaruan Sebelumnya 16332
..... 16402

Apa itu AWS Config?

AWS Config memberikan tampilan terperinci tentang konfigurasi AWS sumber daya di AWS akun Anda. Ini mencakup bagaimana sumber daya terkait satu sama lain dan bagaimana sumber daya tersebut dikonfigurasi di masa lalu sehingga Anda dapat melihat bagaimana konfigurasi dan hubungan berubah dari waktu ke waktu.

AWS Resource adalah entitas yang dapat Anda gunakan AWS, seperti instans Amazon Elastic Compute Cloud (EC2), volume Amazon Elastic Block Store (EBS), grup keamanan, atau Amazon Virtual Private Cloud (VPC). Untuk daftar lengkap AWS sumber daya yang didukung oleh AWS Config, lihatJenis Sumber Daya yang Didukung untuk AWS Config.

Pertimbangan

- Akun AWS: Anda membutuhkan yang aktif Akun AWS. Untuk informasi selengkapnya, lihat Mendaftar untuk AWS.
- Amazon S3 Bucket: Anda memerlukan bucket S3 untuk menerima data untuk snapshot dan riwayat konfigurasi Anda. Untuk informasi selengkapnya, lihat Izin untuk Bucket Amazon S3.
- Topik Amazon SNS: Anda memerlukan Amazon SNS untuk menerima pemberitahuan ketika ada perubahan pada snapshot dan riwayat konfigurasi Anda. Untuk informasi selengkapnya, lihat Izin untuk Topik Amazon SNS.
- Peran IAM: Anda memerlukan peran IAM yang memiliki izin yang diperlukan untuk mengakses. AWS Config Untuk informasi selengkapnya, lihat Izin untuk Peran IAM.
- Jenis sumber daya: Anda dapat memutuskan jenis sumber daya yang AWS Config ingin Anda rekam. Untuk informasi selengkapnya, lihat Merekam AWS Sumber Daya.

Cara Menggunakan AWS Config

Ketika Anda menjalankan aplikasi Anda AWS, Anda biasanya menggunakan AWS sumber daya, yang harus Anda buat dan kelola secara kolektif. Karena permintaan untuk aplikasi Anda terus meningkat, begitu juga kebutuhan Anda untuk melacak sumber AWS daya Anda. AWS Config dirancang untuk membantu Anda mengawasi sumber daya aplikasi Anda dalam skenario berikut:

Administrasi Sumber Daya

Untuk menjalankan tata kelola yang lebih baik atas konfigurasi sumber daya Anda dan untuk mendeteksi kesalahan konfigurasi sumber daya, Anda memerlukan visibilitas terperinci tentang sumber daya apa yang ada dan bagaimana sumber daya ini dikonfigurasi kapan saja. Anda dapat menggunakannya AWS Config untuk memberi tahu Anda setiap kali sumber daya dibuat, dimodifikasi, atau dihapus tanpa harus memantau perubahan ini dengan melakukan polling panggilan yang dilakukan ke setiap sumber daya.

Anda dapat menggunakan AWS Config aturan untuk mengevaluasi pengaturan konfigurasi AWS sumber daya Anda. Saat AWS Config mendeteksi bahwa sumber daya melanggar ketentuan di salah satu aturan Anda, AWS Config tandai sumber daya sebagai tidak sesuai dan mengirimkan pemberitahuan. AWS Config terus mengevaluasi sumber daya Anda saat dibuat, diubah, atau dihapus.

Audit dan Kepatuhan

Anda mungkin bekerja dengan data yang memerlukan audit yang sering untuk memastikan kepatuhan terhadap kebijakan internal dan praktik terbaik. Untuk menunjukkan kepatuhan, Anda memerlukan akses ke konfigurasi historis sumber daya Anda. Informasi ini disediakan oleh AWS Config.

Mengelola dan Memecahkan Masalah Perubahan Konfigurasi

Bila Anda menggunakan beberapa AWS sumber daya yang bergantung satu sama lain, perubahan konfigurasi satu sumber daya mungkin memiliki konsekuensi yang tidak diinginkan pada sumber daya terkait. Dengan AWS Config, Anda dapat melihat bagaimana sumber daya yang ingin Anda modifikasi terkait dengan sumber daya lain dan menilai dampak perubahan Anda.

Anda juga dapat menggunakan konfigurasi historis sumber daya Anda yang disediakan oleh AWS Config untuk memecahkan masalah dan mengakses konfigurasi sumber daya masalah yang terakhir diketahui.

Analisis Keamanan

Untuk menganalisis potensi kelemahan keamanan, Anda memerlukan informasi historis terperinci tentang konfigurasi AWS sumber daya Anda, seperti izin AWS Identity and Access Management (IAM) yang diberikan kepada pengguna Anda, atau aturan grup EC2 keamanan Amazon yang mengontrol akses ke sumber daya Anda.

Anda dapat menggunakan AWS Config untuk melihat kebijakan IAM yang ditetapkan ke pengguna, grup, atau peran kapan saja AWS Config yang merekam. Informasi ini dapat membantu Anda menentukan izin yang dimiliki pengguna pada waktu tertentu: misalnya, Anda dapat melihat apakah pengguna `John Doe` memiliki izin untuk mengubah pengaturan VPC Amazon pada 1 Januari 2015.

Anda juga dapat menggunakan AWS Config untuk melihat konfigurasi grup EC2 keamanan Anda, termasuk aturan port yang terbuka pada waktu tertentu. Informasi ini dapat membantu Anda menentukan apakah grup keamanan memblokir lalu lintas TCP yang masuk ke port tertentu.

Solusi Mitra

AWS bermitra dengan spesialis pihak ketiga dalam pencatatan dan analisis untuk memberikan solusi yang menggunakan AWS Config output. Untuk informasi lebih lanjut, kunjungi halaman AWS Config detail di AWS Config.

Fitur

Saat Anda mengatur AWS Config, Anda dapat menyelesaikan yang berikut ini:

Manajemen sumber daya

- Tentukan jenis sumber daya yang AWS Config ingin Anda rekam.

- Siapkan bucket Amazon S3 untuk menerima snapshot konfigurasi berdasarkan permintaan dan riwayat konfigurasi.
- Siapkan Amazon SNS untuk mengirim pemberitahuan aliran konfigurasi.
- Berikan izin AWS Config yang diperlukan untuk mengakses bucket Amazon S3 dan topik Amazon SNS.

  Untuk informasi selengkapnya, lihat Melihat Konfigurasi AWS Sumber Daya dan Riwayat serta Mengelola Konfigurasi dan Riwayat AWS Sumber Daya.

Aturan dan paket kesesuaian

- Tentukan aturan yang ingin Anda gunakan AWS Config untuk mengevaluasi informasi kepatuhan untuk jenis sumber daya yang direkam.
- Gunakan paket kesesuaian, atau kumpulan aturan yang dapat diterapkan dan dipantau sebagai satu entitas di Anda. Akun AWS

Untuk informasi selengkapnya, lihat Mengevaluasi Sumber Daya dengan AWS Config Aturan dan Paket Kesesuaian.

Remediasi

- Memulihkan sumber daya yang tidak patuh yang dievaluasi oleh. Aturan AWS Config

  Untuk informasi lebih lanjut, lihat Remediasi.

Agregator

- Gunakan agregator untuk mendapatkan tampilan terpusat dari inventaris dan kepatuhan sumber daya Anda. Agregator mengumpulkan data AWS Config konfigurasi dan kepatuhan dari beberapa Akun AWS dan AWS Wilayah ke dalam satu akun dan Wilayah.

  Untuk informasi selengkapnya, lihat Agregasi Data Multi-Wilayah Multi-Akun.

Kueri lanjutan

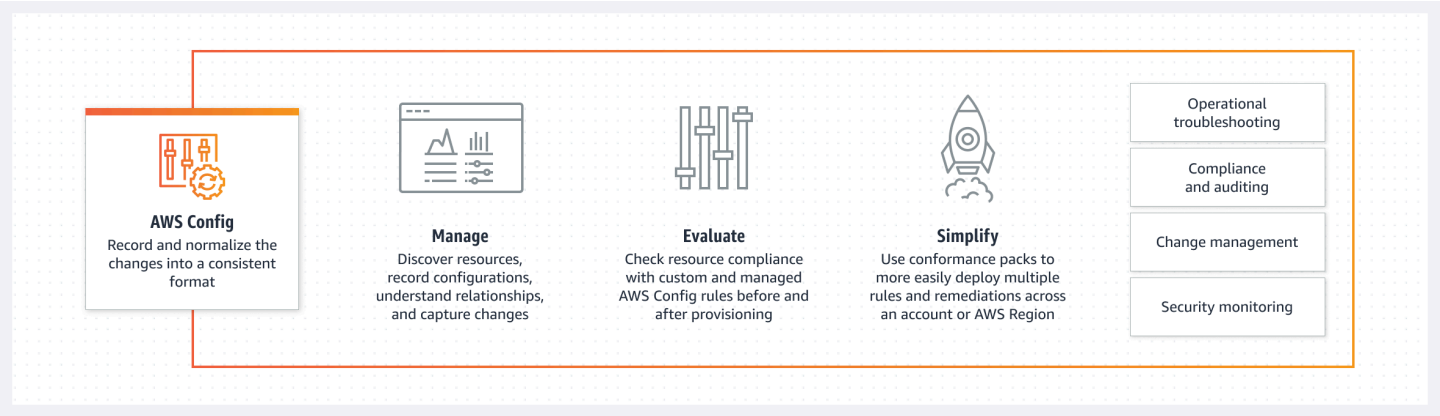
- Gunakan salah satu contoh kueri atau tulis kueri Anda sendiri dengan mengacu pada skema konfigurasi sumber daya. AWS

  Untuk informasi selengkapnya, lihat Menanyakan Status AWS Sumber Daya Konfigurasi Saat Ini.

Cara AWS Config Kerja

AWS Config memberikan tampilan terperinci tentang konfigurasi AWS sumber daya di AWS akun Anda. Ini mencakup bagaimana sumber daya terkait satu sama lain dan bagaimana sumber daya tersebut dikonfigurasi di masa lalu sehingga Anda dapat melihat bagaimana konfigurasi dan hubungan berubah dari waktu ke waktu.

AWS Resource adalah entitas yang dapat Anda gunakan AWS, seperti instans Amazon Elastic Compute Cloud (EC2), volume Amazon Elastic Block Store (EBS), grup keamanan, atau Amazon Virtual Private Cloud (VPC). Untuk daftar lengkap AWS sumber daya yang didukung oleh AWS Config, lihatJenis Sumber Daya yang Didukung untuk AWS Config.



Penemuan Sumber Daya

Saat Anda mengaktifkan AWS Config, pertama kali menemukan AWS sumber daya yang didukung yang ada di akun Anda dan menghasilkan item konfigurasi untuk setiap sumber daya.

AWS Config juga menghasilkan item konfigurasi saat konfigurasi sumber daya berubah, dan menyimpan catatan historis item konfigurasi sumber daya Anda sejak Anda memulai perekam konfigurasi. Secara default, AWS Config membuat item konfigurasi untuk setiap sumber daya yang didukung di wilayah tersebut. Jika Anda tidak AWS Config ingin membuat item konfigurasi untuk semua sumber daya yang didukung, Anda dapat menentukan jenis sumber daya yang ingin dilacak.

Sebelum menentukan jenis sumber daya AWS Config untuk dilacak, periksa Cakupan Sumber Daya menurut Ketersediaan Wilayah untuk melihat apakah jenis sumber daya didukung di AWS Wilayah tempat Anda menyiapkan AWS Config. Jika jenis sumber daya didukung oleh AWS Config setidaknya satu Wilayah, Anda dapat mengaktifkan perekaman jenis sumber daya tersebut di semua Wilayah yang didukung oleh AWS Config, meskipun jenis sumber daya yang ditentukan tidak didukung AWS Wilayah tempat Anda menyiapkan AWS Config.

Pelacakan Sumber Daya

AWS Config melacak semua perubahan pada sumber daya Anda dengan menjalankan panggilan Deskripsikan atau API Daftar untuk setiap sumber daya di akun Anda. Layanan ini menggunakan panggilan API yang sama untuk menangkap detail konfigurasi untuk semua sumber daya terkait.

Misalnya, menghapus aturan keluar dari grup keamanan VPC menyebabkan AWS Config panggilan Deskripsikan API di grup keamanan. AWS Config kemudian memanggil panggilan Describe API pada semua instance yang terkait dengan grup keamanan. Konfigurasi terbaru grup keamanan (sumber daya) dan setiap instance (sumber daya terkait) direkam sebagai item konfigurasi dan dikirimkan dalam aliran konfigurasi ke bucket Amazon Simple Storage Service (Amazon S3).

AWS Config juga melacak perubahan konfigurasi yang tidak diprakarsai oleh API. AWS Config memeriksa konfigurasi sumber daya secara berkala dan menghasilkan item konfigurasi untuk konfigurasi yang telah berubah.

Jika Anda menggunakan AWS Config aturan, AWS Config terus mengevaluasi konfigurasi AWS sumber daya Anda untuk pengaturan yang diinginkan. Tergantung pada aturan, AWS Config akan mengevaluasi sumber daya Anda baik dalam menanggapi perubahan konfigurasi atau secara berkala. Setiap aturan dikaitkan dengan AWS Lambda fungsi, yang berisi logika evaluasi untuk aturan tersebut. Ketika AWS Config mengevaluasi sumber daya Anda, itu memanggil fungsi aturan. AWS Lambda Fungsi mengembalikan status kepatuhan sumber daya yang dievaluasi. Jika sumber daya melanggar ketentuan aturan, AWS Config tandai sumber daya dan aturan sebagai tidak patuh. Saat status kepatuhan sumber daya berubah, AWS Config kirimkan pemberitahuan ke topik Amazon SNS Anda.

Pengiriman Item Konfigurasi

AWS Config dapat mengirimkan item konfigurasi melalui salah satu saluran berikut:

Bucket Amazon S3

AWS Config melacak perubahan dalam konfigurasi AWS sumber daya Anda, dan secara teratur mengirimkan detail konfigurasi yang diperbarui ke bucket Amazon S3 yang Anda tentukan. Untuk setiap jenis sumber daya yang AWS Config merekam, ia mengirimkan file riwayat konfigurasi setiap enam jam. Setiap file riwayat konfigurasi berisi detail tentang sumber daya yang berubah dalam periode enam jam itu. Setiap file menyertakan sumber daya dari satu jenis, seperti EC2 instans Amazon atau volume Amazon EBS. Jika tidak ada perubahan konfigurasi yang terjadi, AWS Config tidak mengirim file.

AWS Config mengirimkan snapshot konfigurasi ke bucket Amazon S3 saat Anda menggunakan perintah deliver-config-snapshotdengan AWS CLI, atau saat Anda menggunakan DeliverConfigSnapshottindakan dengan API. AWS Config Snapshot konfigurasi berisi detail konfigurasi untuk semua sumber daya yang AWS Config merekam dalam file Anda Akun AWS. File riwayat konfigurasi dan snapshot konfigurasi dalam format JSON.

> **Note**
>
> AWS Config hanya mengirimkan file riwayat konfigurasi dan snapshot konfigurasi ke bucket S3 yang ditentukan; AWS Config tidak mengubah kebijakan siklus hidup untuk objek di bucket S3. Anda dapat menggunakan kebijakan siklus hidup untuk menentukan apakah

Anda ingin menghapus atau mengarsipkan objek ke Amazon S3 Glacier. Untuk informasi selengkapnya, lihat Mengelola Konfigurasi Siklus Hidup di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon. Anda juga dapat melihat Pengarsipan Data Amazon S3 ke posting blog S3 Glacier.

Topik Amazon SNS

Topik Amazon Simple Notification Service (Amazon SNS) adalah saluran komunikasi yang digunakan Amazon SNS untuk mengirimkan pesan (atau notifikasi) ke titik akhir berlangganan seperti alamat email atau klien. Jenis notifikasi Amazon SNS lainnya termasuk pesan pemberitahuan push ke aplikasi di ponsel, pemberitahuan Layanan Pesan Singkat (SMS) ke ponsel dan ponsel pintar berkemampuan SMS, dan permintaan HTTP POST. Untuk hasil terbaik, gunakan Amazon SQS sebagai titik akhir notifikasi untuk topik SNS dan kemudian proses informasi dalam notifikasi secara terprogram.

AWS Config menggunakan topik Amazon SNS yang Anda tentukan untuk mengirimi Anda pemberitahuan. Jenis notifikasi yang Anda terima ditunjukkan oleh nilai `messageType` kunci di badan pesan, seperti pada contoh berikut:

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

Pemberitahuan dapat berupa salah satu jenis pesan berikut.

Jenis pesan	Deskripsi
ComplianceChangeNotification	Jenis kepatuhan sumber daya yang AWS Config mengevaluasi telah berubah. Jenis kepatuhan menunjukkan apakah sumber daya mematuhi AWS Config aturan tertentu, dan diwakili oleh `ComplianceType` kunci dalam pesan. Pesan termasuk `newEvaluationResult` dan `oldEvaluationResult` objek untuk perbandingan.
ConfigRulesEvaluationStarted	AWS Config mulai mengevaluasi aturan Anda terhadap sumber daya yang ditentukan.

Jenis pesan	Deskripsi
ConfigurationSnapshotDeliveryStarted	AWS Config mulai mengirimkan snapshot konfigurasi ke bucket Amazon S3 Anda. Nama bucket Amazon S3 disediakan untuk `s3Bucket` kunci dalam pesan.
ConfigurationSnapshotDeliveryCompleted	AWS Config berhasil mengirimkan snapshot konfigurasi ke bucket Amazon S3 Anda.
ConfigurationSnapshotDeliveryFailed	AWS Config gagal mengirimkan snapshot konfigurasi ke bucket Amazon S3 Anda.
ConfigurationHistoryDeliveryCompleted	AWS Config berhasil mengirimkan riwayat konfigurasi ke bucket Amazon S3 Anda.
ConfigurationItemChangeNotification	Sumber daya telah dibuat, dihapus, atau diubah dalam konfigurasi. Pesan ini mencakup detail item konfigurasi yang AWS Config dibuat untuk perubahan ini, dan itu termasuk jenis perubahan. Pemberitahuan ini dikirimkan dalam beberapa menit setelah perubahan dan secara kolektif dikenal sebagai aliran konfigurasi.
OversizedConfigurationItemChangeNotification	Jenis pesan ini dikirimkan ketika pemberita huan perubahan item konfigurasi melebihi ukuran maksimum yang diizinkan oleh Amazon SNS. Pesan tersebut mencakup ringkasan item konfigurasi. Dengan pengecualian pesan SMS, pesan Amazon SNS dapat berisi hingga 256 KB data teks, termasuk XHTML, JSON, dan teks yang tidak diformat. Anda dapat melihat notifikasi lengkap di lokasi bucket Amazon S3 yang ditentukan.
OversizedConfigurationItemChangeDeli veryFailed	AWS Config gagal mengirimkan pemberitahuan perubahan item konfigurasi berukuran besar ke bucket Amazon S3 Anda.

Misalnya notifikasi, lihatPemberitahuan yang AWS Config Mengirim ke topik Amazon SNS. Untuk informasi selengkapnya tentang Amazon SNS, lihat Panduan Developer Amazon Simple Notification Service.

> **Note**
>
> Mengapa saya tidak dapat melihat perubahan konfigurasi terbaru saya?
> AWS Config biasanya mencatat perubahan konfigurasi ke sumber daya Anda tepat setelah perubahan terdeteksi, atau pada frekuensi yang Anda tentukan. Namun, ini atas dasar upaya terbaik dan kadang-kadang bisa memakan waktu lebih lama. Jika masalah berlanjut setelah beberapa waktu, hubungi Dukungandan berikan AWS Config metrik Anda yang didukung oleh Amazon. CloudWatch Untuk informasi tentang metrik ini, lihat Metrik AWS Config Penggunaan dan Sukses.

Kontrol Akses ke AWS Config

AWS Identity and Access Management adalah layanan web yang memungkinkan pelanggan Amazon Web Services (AWS) untuk mengelola pengguna dan izin pengguna.

Untuk memberikan akses dan menambahkan izin bagi pengguna, grup, atau peran Anda:

- Pengguna dan grup di AWS IAM Identity Center:

  Buat rangkaian izin. Ikuti instruksi di Buat rangkaian izin di Panduan Pengguna AWS IAM Identity Center .

- Pengguna yang dikelola di IAM melalui penyedia identitas:

  Buat peran untuk federasi identitas. Ikuti instruksi dalam Buat peran untuk penyedia identitas pihak ketiga (federasi) dalam Panduan Pengguna IAM.

- Pengguna IAM:
  - Buat peran yang dapat diambil pengguna Anda. Ikuti instruksi dalam Buat peran untuk pengguna IAM dalam Panduan Pengguna IAM.
  - (Tidak disarankan) Lampirkan kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti petunjuk dalam Menambahkan izin ke pengguna (konsol) dalam Panduan Pengguna IAM.

AWS Config terminologi dan konsep

Untuk membantu Anda memahami AWS Config, topik ini menjelaskan beberapa konsep kunci.

Daftar Isi

- AWS Config Antarmuka
  - AWS Config Konsol
  - AWS Config CLI
  - AWS Config APIs
  - AWS Config SDKs
- Manajemen Sumber Daya
  - AWS Sumber Daya
  - Hubungan Sumber Daya
- Pencatat Konfigurasi
- Saluran Pengiriman
  - Item Konfigurasi
  - Riwayat Konfigurasi
  - Snapshot Konfigurasi
  - Aliran Konfigurasi
- AWS Config Aturan
  - Hasil Evaluasi
  - Jenis Aturan
  - Jenis Pemicu
  - Mode evaluasi
- Paket Kesesuaian
- Agregasi Data Multi-Wilayah Multi-Akun
  - Akun Sumber
  - Wilayah Sumber
  - Agregator
  - Agregator terkait layanan
  - Akun Agregator

- Otorisasi

AWS Config Antarmuka

AWS Config Konsol

Anda dapat mengelola layanan menggunakan AWS Config konsol. Untuk informasi lebih lanjut tentang AWS Management Console, lihat AWS Management Console.

AWS Config CLI

AWS Command Line Interface Ini adalah alat terpadu yang dapat Anda gunakan untuk berinteraksi AWS Config dari baris perintah. Untuk informasi selengkapnya, lihat Panduan Pengguna AWS Command Line Interface. Untuk daftar lengkap perintah AWS Config CLI, lihat Perintah yang Tersedia.

AWS Config APIs

Selain konsol dan CLI, Anda juga dapat menggunakan program AWS Config RESTful APIs AWS Config to secara langsung. Untuk informasi lebih lanjut, lihat Referensi API AWS Config.

AWS Config SDKs

Sebagai alternatif untuk menggunakan AWS Config API, Anda dapat menggunakan salah satu dari AWS SDKs. Setiap SDK terdiri dari pustaka dan kode sampel untuk berbagai bahasa dan platform pemrograman. SDKs Menyediakan cara mudah untuk membuat akses terprogram ke AWS Config. Misalnya, Anda dapat menggunakan SDKs untuk menandatangani permintaan secara kriptografis, mengelola kesalahan, dan mencoba ulang permintaan secara otomatis. Untuk informasi selengkapnya, lihat halaman Alat untuk Amazon Web Services.

Manajemen Sumber Daya

Memahami komponen dasar AWS Config akan membantu Anda melacak inventaris sumber daya dan perubahan serta mengevaluasi konfigurasi AWS sumber daya Anda.

AWS Sumber Daya

AWS sumber daya adalah entitas yang Anda buat dan kelola menggunakan AWS Management Console, AWS Command Line Interface (CLI), alat AWS SDKs, atau AWS mitra. Contoh sumber AWS daya termasuk EC2 instans Amazon, grup keamanan, Amazon VPCs, dan Amazon Elastic

Block Store. AWS Config mengacu pada setiap sumber daya menggunakan pengenal uniknya, seperti ID sumber daya atau Nama Sumber Daya Amazon (ARN). Untuk daftar jenis sumber daya yang AWS Config mendukung, lihatJenis Sumber Daya yang Didukung untuk AWS Config.

Hubungan Sumber Daya

AWS Config menemukan AWS sumber daya di akun Anda dan kemudian membuat peta hubungan antar AWS sumber daya. Misalnya, hubungan mungkin menyertakan volume Amazon EBS yang `vol-123ab45d` dilampirkan ke EC2 instans Amazon `i-a1b2c3d4` yang terkait dengan grup `sg-ef678hk` keamanan.

Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.

Pencatat Konfigurasi

Perekam konfigurasi menyimpan perubahan konfigurasi pada jenis sumber daya dalam lingkup sebagai item konfigurasi. Untuk informasi selengkapnya, lihat Bekerja dengan perekam konfigurasi.

Ada dua jenis perekam konfigurasi.

Jenis	Deskripsi
Perekam konfigurasi terkelola pelanggan	Perekam konfigurasi yang Anda kelola. Jenis sumber daya dalam lingkup ditetapkan oleh Anda. Secara default, perekam konfigurasi terkelola pelanggan merekam semua sumber daya yang AWS Config didukung Wilayah AWS di tempat berjalan.
Perekam konfigurasi terkait layanan	Perekam konfigurasi yang ditautkan ke yang spesifik Layanan AWS. Jenis sumber daya dalam lingkup ditetapkan oleh layanan tertaut.

Saluran Pengiriman

Karena AWS Config terus-menerus mencatat perubahan yang terjadi pada AWS sumber daya Anda, ia mengirimkan pemberitahuan dan status konfigurasi yang diperbarui melalui saluran pengiriman. Anda dapat mengelola saluran pengiriman untuk mengontrol tempat AWS Config mengirim pembaruan konfigurasi.

Item Konfigurasi

Item konfigurasi mewakili point-in-time tampilan berbagai atribut AWS sumber daya yang didukung yang ada di akun Anda. Komponen item konfigurasi termasuk metadata, atribut, hubungan, konfigurasi saat ini, dan peristiwa terkait. AWS Config membuat item konfigurasi setiap kali mendeteksi perubahan pada jenis sumber daya yang direkam. Misalnya, jika AWS Config merekam bucket Amazon S3, AWS Config buat item konfigurasi setiap kali bucket dibuat, diperbarui, atau dihapus. Anda juga dapat memilih AWS Config untuk membuat item konfigurasi pada frekuensi perekaman yang Anda atur.

Untuk informasi lebih lanjut, lihat Components of a Configuration Item dan Frekuensi Perekaman.

Riwayat Konfigurasi

Riwayat konfigurasi adalah kumpulan item konfigurasi untuk sumber daya tertentu selama periode waktu apa pun. Riwayat konfigurasi dapat membantu Anda menjawab pertanyaan tentang, misalnya, kapan sumber daya pertama kali dibuat, bagaimana sumber daya telah dikonfigurasi selama sebulan terakhir, dan perubahan konfigurasi apa yang diperkenalkan kemarin pukul 9 pagi. Riwayat konfigurasi tersedia untuk Anda dalam berbagai format. AWS Config secara otomatis mengirimkan file riwayat konfigurasi untuk setiap jenis sumber daya yang direkam ke bucket Amazon S3 yang Anda tentukan. Anda dapat memilih sumber daya tertentu di AWS Config konsol dan menavigasi ke semua item konfigurasi sebelumnya untuk sumber daya tersebut menggunakan timeline. Selain itu, Anda dapat mengakses item konfigurasi historis untuk sumber daya dari API.

Untuk informasi selengkapnya, lihat Melihat Riwayat Kepatuhan dan Meminta Riwayat Kepatuhan.

Snapshot Konfigurasi

Snapshot konfigurasi adalah kumpulan item konfigurasi untuk sumber daya yang didukung yang ada di akun Anda. Snapshot konfigurasi ini adalah gambaran lengkap dari sumber daya yang sedang direkam dan konfigurasinya. Snapshot konfigurasi dapat menjadi alat yang berguna untuk memvalidasi konfigurasi Anda. Misalnya, Anda mungkin ingin memeriksa snapshot konfigurasi secara teratur untuk sumber daya yang dikonfigurasi secara tidak benar atau yang berpotensi tidak ada. Snapshot konfigurasi tersedia dalam berbagai format. Snapshot konfigurasi dapat dikirimkan ke bucket Amazon Simple Storage Service (Amazon S3) yang ditentukan. Selain itu, Anda dapat memilih titik waktu di AWS Config konsol dan menavigasi snapshot item konfigurasi menggunakan hubungan antar sumber daya.

Untuk informasi selengkapnya, lihat Menyampaikan Snapshot Konfigurasi, Melihat Snapshot Konfigurasi, dan Contoh Snapshot Konfigurasi.

Aliran Konfigurasi

Aliran konfigurasi adalah daftar yang diperbarui secara otomatis dari semua item konfigurasi untuk sumber daya AWS Config yang direkam. Setiap kali sumber daya dibuat, dimodifikasi, atau dihapus, AWS Config buat item konfigurasi dan tambahkan ke aliran konfigurasi. Aliran konfigurasi berfungsi dengan menggunakan topik Amazon Simple Notification Service (Amazon SNS) pilihan Anda. Aliran konfigurasi sangat membantu untuk mengamati perubahan konfigurasi saat terjadi sehingga Anda dapat menemukan potensi masalah, menghasilkan pemberitahuan jika sumber daya tertentu diubah, atau memperbarui sistem eksternal yang perlu mencerminkan konfigurasi sumber AWS daya Anda.

AWS Config Aturan

AWS Config Aturan adalah pemeriksaan kepatuhan yang membantu Anda mengelola pengaturan konfigurasi ideal untuk AWS sumber daya tertentu. AWS Config mengevaluasi apakah konfigurasi sumber daya Anda mematuhi aturan yang relevan dan menampilkan hasil kepatuhan.

Hasil Evaluasi

Ada empat kemungkinan hasil evaluasi untuk suatu AWS Config aturan.

Hasil evaluasi	Deskripsi
`COMPLIANT`	Aturan melewati kondisi pemeriksaan kepatuhan.
`NON_COMPLIANT`	Aturan gagal dalam kondisi pemeriksaan kepatuhan.
`ERROR`	Salah satu parameter yang diperlukan/opsional tidak valid, bukan dari jenis yang benar, atau diformat secara tidak benar.
`NOT_APPLICABLE`	Digunakan untuk menyaring sumber daya yang logika aturan tidak dapat diterapkan. Misalnya, alb-desync-mode-checkaturan hanya memeriksa Application Load Balancers, dan mengabaikan Network Load Balancers dan Gateway Load Balancers.

Jenis Aturan

Ada dua jenis aturan. Untuk informasi selengkapnya tentang struktur definisi aturan dan metadata aturan, lihat Komponen Aturan. AWS Config

Jenis	Deskripsi	Informasi lebih lanjut
Aturan terkelola	Aturan yang telah ditentukan dan dapat disesuaikan yang dibuat oleh. AWS Config	Untuk daftar aturan terkelola , lihat Daftar Aturan AWS Config Terkelola.
Aturan kustom	Aturan yang Anda buat dari awal. Ada dua cara untuk membuat aturan AWS Config khusus: fungsi Lambda (Panduan AWS Lambda Pengembang) dan Penjaga (Repositori Penjaga GitHub)	Untuk selengkapnya, lihat Membuat Aturan Kebijakan AWS Config Kustom dan Membuat Aturan Lambda AWS Config Kustom.

Jenis Pemicu

Setelah Anda menambahkan aturan ke akun Anda, AWS Config bandingkan sumber daya Anda dengan ketentuan aturan. Setelah evaluasi awal ini, AWS Config terus jalankan evaluasi setiap kali dipicu. Pemicu evaluasi didefinisikan sebagai bagian dari aturan, dan mereka dapat mencakup jenis berikut.

Jenis pemicu	Deskripsi
Perubahan konfigurasi	AWS Config menjalankan evaluasi untuk aturan ketika ada sumber daya yang cocok dengan cakupan aturan dan ada perubahan konfigura si sumber daya. Evaluasi berjalan setelah AWS Config mengirimkan pemberitahuan perubahan item konfigurasi. Anda memilih sumber daya mana yang memulai evaluasi dengan menentukan ruang

Jenis pemicu	Deskripsi
	lingkup aturan. Ruang lingkup dapat mencakup yang berikut: • Satu atau lebih jenis sumber daya • Kombinasi tipe sumber daya dan ID sumber daya • Kombinasi kunci tag dan nilai • Ketika sumber daya yang direkam dibuat, diperbarui, atau dihapus AWS Config menjalankan evaluasi saat mendeteksi perubahan pada sumber daya yang cocok dengan cakupan aturan. Anda dapat menggunakan ruang lingkup untuk menentukan sumber daya mana yang memulai evaluasi.
Berkala	AWS Config menjalankan evaluasi untuk aturan pada frekuensi yang Anda pilih; misalnya, setiap 24 jam.
Hibrida	Beberapa aturan memiliki perubahan konfigura si dan pemicu periodik. Untuk aturan ini, AWS Config evaluasi sumber daya Anda saat mendeteksi perubahan konfigurasi dan juga pada frekuensi yang Anda tentukan.

Mode evaluasi

Ada dua mode evaluasi untuk AWS Config aturan.

Mode evaluasi	Deskripsi
Proaktif	Gunakan evaluasi proaktif untuk mengevalu asi sumber daya sebelum digunakan. Ini memungkinkan Anda untuk mengevaluasi

Mode evaluasi	Deskripsi
	apakah satu set properti sumber daya, jika digunakan untuk mendefinisikan AWS sumber daya, akan COMPLIANT atau NON_COMPL IANT mengingat seperangkat aturan proaktif yang Anda miliki di akun Anda di Wilayah Anda. Untuk informasi selengkapnya, lihat Mode evaluasi. Untuk daftar aturan terkelola yang mendukung evaluasi proaktif, lihat Daftar Aturan AWS Config Terkelola menurut Mode Evaluasi.
Detective	Gunakan evaluasi detektif untuk mengevalu asi sumber daya yang telah digunakan. Ini memungkinkan Anda untuk mengevaluasi pengaturan konfigurasi sumber daya yang ada.

> **Note**
>
> Aturan proaktif tidak memulihkan sumber daya yang ditandai sebagai NON_COMPLIANT atau mencegahnya diterapkan.

Paket Kesesuaian

Paket kesesuaian adalah kumpulan AWS Config aturan dan tindakan remediasi yang dapat dengan mudah digunakan sebagai entitas tunggal dalam akun dan Wilayah atau di seluruh organisasi di. AWS Organizations

Paket kesesuaian dibuat dengan membuat template YAMB yang berisi daftar aturan AWS Config terkelola atau kustom dan tindakan remediasi. Anda dapat menerapkan template dengan menggunakan AWS Config konsol atau file. AWS CLI

Untuk memulai dengan cepat dan mengevaluasi AWS lingkungan Anda, gunakan salah satu contoh templat paket kesesuaian. Anda juga dapat membuat paket kesesuaian file YAMG dari awal berdasarkan Paket Kesesuaian Kustom. Paket kesesuaian kustom adalah kumpulan AWS Config

aturan dan tindakan remediasi unik yang dapat Anda terapkan bersama di akun dan AWS Wilayah, atau di seluruh organisasi di. AWS Organizations

Pemeriksaan proses adalah jenis AWS Config aturan yang memungkinkan Anda melacak tugas eksternal dan internal Anda yang memerlukan verifikasi sebagai bagian dari paket kesesuaian. Pemeriksaan ini dapat ditambahkan ke paket kesesuaian yang ada atau paket kesesuaian baru. Anda dapat melacak semua kepatuhan yang mencakup AWS Config urasi dan pemeriksaan manual di satu lokasi.

Agregasi Data Multi-Wilayah Multi-Akun

Agregasi data multi-wilayah multi-akun AWS Config memungkinkan Anda untuk menggabungkan AWS Config konfigurasi dan data kepatuhan dari beberapa akun dan wilayah ke dalam satu akun. Agregasi data multi-wilayah multi-akun berguna bagi administrator TI pusat untuk memantau kepatuhan untuk beberapa Akun AWS di perusahaan. Menggunakan agregator tidak menimbulkan biaya tambahan.

Akun Sumber

Akun sumber adalah Akun AWS dari mana Anda ingin menggabungkan konfigurasi AWS Config sumber daya dan data kepatuhan. Akun sumber dapat berupa akun individu atau organisasi di AWS Organizations. Anda dapat memberikan akun sumber satu per satu atau Anda dapat mengambilnya. AWS Organizations

Wilayah Sumber

Wilayah sumber adalah AWS Wilayah tempat Anda ingin menggabungkan AWS Config konfigurasi dan data kepatuhan.

Agregator

Agregator mengumpulkan data AWS Config konfigurasi dan kepatuhan dari beberapa akun sumber dan wilayah. Buat agregator di wilayah tempat Anda ingin melihat AWS Config konfigurasi gabungan dan data kepatuhan.

> **Note**
>
> Agregator menyediakan tampilan hanya-baca ke dalam akun sumber dan wilayah yang agregator berwenang untuk melihat dengan mereplikasi data dari akun sumber ke akun agregator. Agregator tidak menyediakan akses bermutasi ke akun sumber atau wilayah.

Misalnya, ini berarti Anda tidak dapat menerapkan aturan melalui agregator atau mendorong file snapshot ke akun sumber atau wilayah melalui agregator.

Agregator terkait layanan

Agregator terkait layanan ditautkan ke yang spesifik. Layanan AWS Konfigurasi dan data kepatuhan dalam lingkup ditetapkan oleh layanan tertaut.

Akun Agregator

Akun agregator adalah akun tempat Anda membuat agregator.

Otorisasi

Sebagai pemilik akun sumber, otorisasi mengacu pada izin yang Anda berikan ke akun agregator dan wilayah untuk mengumpulkan data AWS Config konfigurasi dan kepatuhan Anda. Otorisasi tidak diperlukan jika Anda menggabungkan akun sumber yang merupakan bagian dari. AWS Organizations

AWS Integrasi Layanan dengan AWS Config

AWS Config mendukung integrasi dengan beberapa AWS layanan lainnya. Daftar ini tidak lengkap.

AWS Organizations

Anda dapat menggunakan AWS Organizations untuk menentukan akun yang akan digunakan untuk AWS Config kemampuan agregasi data multi-akun dan Multi-wilayah. AWS Organizations adalah layanan manajemen akun yang membantu Anda mengkonsolidasikan beberapa Akun AWS ke dalam organisasi yang Anda buat dan kelola secara terpusat. Dengan memberikan AWS Organizations detail, Anda dapat memantau status kepatuhan di seluruh organisasi Anda. Untuk informasi lebih lanjut, AWS Config dan AWS Organizations di Panduan AWS Organizations Pengguna.

AWS Control Tower

AWS Control Tower memungkinkan AWS Config pada semua akun yang terdaftar, sehingga dapat memantau kepatuhan melalui kontrol detektif, merekam perubahan sumber daya, dan mengirimkan log perubahan sumber daya ke akun arsip log. Untuk informasi selengkapnya, lihat Memantau perubahan sumber daya AWS Config di Panduan AWS Control Tower Pengguna.

AWS CloudTrail

AWS Config terintegrasi dengan AWS CloudTrail untuk mengkorelasikan perubahan konfigurasi dengan peristiwa tertentu di akun Anda. Anda dapat menggunakan CloudTrail log untuk mendapatkan rincian peristiwa yang memanggil perubahan, termasuk siapa yang membuat permintaan, pada jam berapa, dan dari alamat IP mana. Anda dapat menavigasi ke AWS Config timeline dari CloudTrail konsol untuk melihat perubahan konfigurasi yang terkait dengan aktivitas AWS API Anda.

Untuk informasi selengkapnya, lihat Mencatat Panggilan AWS Config API dengan AWS CloudTrail di Panduan AWS Config Pengembang dan Membuat penyimpanan data peristiwa untuk item AWS Config konfigurasi dengan konsol di Panduan AWS CloudTrail Pengguna.

AWS Security Hub

AWS Security Hub memusatkan pemeriksaan keamanan dari AWS layanan lain, termasuk AWS Config aturan. Security Hub mengaktifkan dan mengontrol AWS Config aturan untuk memverifikasi konfigurasi sumber daya Anda selaras dengan praktik terbaik. Aktifkan AWS Config pada semua akun di semua Wilayah tempat Security Hub menjalankan pemeriksaan keamanan pada sumber daya lingkungan Anda. Untuk informasi selengkapnya, lihat AWS layanan yang mengirimkan temuan ke Security Hub di Panduan AWS Security Hub Pengguna.

> **Beberapa aturan terkait Hub Keamanan bersifat periodik dan tidak bergantung pada item konfigurasi**
>
> Beberapa aturan terkait Hub Keamanan bersifat periodik. Aturan ini dapat berjalan tanpa perekam konfigurasi diaktifkan dan tidak bergantung pada item konfigurasi (CI).
> Ini berarti bahwa jika Anda melihat halaman aturan, tidak ada CI terdaftar atau sumber daya yang didukung. Jika Anda memilih ID sumber daya, Anda akan melihat kesalahan berikut:`The provided resource ID and resource type cannot be found`. Ini adalah perilaku yang diharapkan.

AWS Trusted Advisor

AWS Config aturan terkelola memberi daya pada serangkaian Trusted Advisor pemeriksaan di semua kategori. Saat Anda mengaktifkan aturan terkelola tertentu, Trusted Advisor pemeriksaan terkait akan diaktifkan secara otomatis. Untuk melihat Trusted Advisor pemeriksaan mana yang

didukung oleh aturan AWS Config terkelola tertentu, lihat AWS Trusted Advisor periksa referensi di Panduan AWS Dukungan Pengguna.

Pemeriksaan AWS Config bertenaga tersedia untuk pelanggan dengan paket AWS Business Support, AWS Enterprise On-Ramp, dan Enterprise AWS Support. Jika Anda mengaktifkan AWS Config dan memiliki salah satu paket AWS Support ini, Anda akan secara otomatis melihat rekomendasi yang didukung oleh aturan AWS Config terkelola yang diterapkan terkait.

> **Permintaan penyegaran tidak diizinkan dan sumber daya tidak dapat dikecualikan**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan berdasarkan pembaruan yang dipicu perubahan pada aturan terkelola. AWS Config Permintaan penyegaran tidak diizinkan. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

Untuk informasi selengkapnya, lihat Melihat Trusted Advisor pemeriksaan yang didukung oleh AWS Config di Panduan AWS Dukungan Pengguna.

AWS Audit Manager

Anda dapat menggunakan Audit Manager untuk menangkap AWS Config evaluasi sebagai bukti audit. Saat membuat atau mengedit kontrol kustom, Anda dapat menentukan satu atau beberapa AWS Config aturan sebagai pemetaan sumber data untuk pengumpulan bukti. AWS Config melakukan pemeriksaan kepatuhan berdasarkan aturan ini, dan Audit Manager melaporkan hasilnya sebagai bukti pemeriksaan kepatuhan. Untuk informasi selengkapnya, lihat AWS Config Aturan yang didukung oleh AWS Audit Manager di Panduan AWS Audit Manager Pengguna.

AWS Systems Manager

AWS Config terintegrasi dengan Systems Manager untuk merekam perubahan konfigurasi ke perangkat lunak di EC2 instans dan server Amazon di lingkungan lokal. Dengan integrasi ini, Anda dapat memperoleh visibilitas ke konfigurasi sistem operasi (OS), pembaruan tingkat sistem, aplikasi yang diinstal, konfigurasi jaringan, dan banyak lagi. AWS Config juga menyediakan riwayat OS dan perubahan konfigurasi tingkat sistem di samping perubahan konfigurasi infrastruktur yang direkam untuk instans Amazon EC2 . Anda dapat menavigasi ke AWS Config timeline dari konsol Systems Manager untuk melihat perubahan konfigurasi EC2 instans Amazon yang dikelola. Anda dapat menggunakan AWS Config untuk melihat riwayat inventaris Systems Manager dan melacak perubahan untuk semua instans terkelola Anda.

Untuk informasi selengkapnya, lihat Integrasi dengan AWS layanan | Manajemen dan Tata Kelola, perekam AWS Config konfigurasi, dan penyebaran paket AWS Config kesesuaian di Panduan Pengguna.AWS Systems Manager

AWS Firewall Manager

Untuk menggunakan Firewall Manager, Anda harus mengaktifkan AWS Config untuk setiap akun AWS Organizations anggota Anda. Ketika aplikasi baru dibuat, Firewall Manager adalah layanan tunggal untuk membangun aturan firewall, membuat kebijakan keamanan, dan menegakkannya secara konsisten. Untuk informasi selengkapnya, lihat Mengaktifkan AWS Config di AWS WAF, AWS Firewall Manager, dan Panduan AWS Shield Advanced Pengembang.

> **Note**
>
> Firewall Manager bergantung pada perekaman berkelanjutan untuk memantau sumber daya Anda. Jika Anda menggunakan Firewall Manager, disarankan agar Anda mengatur frekuensi perekaman ke Continuous. Untuk informasi lebih lanjut tentang perekaman berkelanjutan dan perekaman harian, lihat Frekuensi Perekaman.

Host EC2 Khusus Amazon

AWS Config terintegrasi dengan Host EC2 Khusus Amazon untuk menilai kepatuhan lisensi. AWS Config merekam saat instance diluncurkan, dihentikan, atau dimatikan pada Host Khusus, dan memasangkan informasi ini dengan informasi tingkat host dan instans yang relevan dengan lisensi perangkat lunak, seperti ID Host, Gambar Mesin Amazon (AMI) IDs, jumlah soket, dan inti fisik. Ini membantu Anda menggunakan AWS Config sebagai sumber data untuk pelaporan lisensi Anda. Anda dapat menavigasi ke AWS Config timeline dari konsol Host EC2 Khusus Amazon untuk melihat perubahan konfigurasi Host EC2 Khusus Amazon Anda.

Untuk informasi selengkapnya, lihat Lacak perubahan konfigurasi di Panduan Pengguna Amazon Elastic Compute Cloud untuk Instans Linux atau Lacak perubahan konfigurasi di Panduan Pengguna Amazon Elastic Compute Cloud untuk Instans Windows.

Application Load Balancer

AWS Config terintegrasi dengan layanan Elastic Load Balancing (ELB) untuk merekam perubahan konfigurasi pada Application Load Balancers. AWS Config juga mencakup hubungan dengan grup

EC2 keamanan Amazon terkait, VPCs, dan subnet. Anda dapat menggunakan informasi ini untuk analisis keamanan dan pemecahan masalah. Misalnya, Anda dapat memeriksa grup keamanan mana yang terkait dengan Application Load Balancer Anda kapan saja. Anda dapat menavigasi ke AWS Config timeline dari konsol ELB untuk melihat perubahan konfigurasi Application Load Balancers Anda.

AWS CodeBuild

AWS Config menyediakan inventaris sumber AWS daya Anda dan riwayat perubahan konfigurasi pada sumber daya ini. AWS Config mendukung AWS CodeBuild; sebagai AWS sumber daya, yang berarti layanan dapat melacak CodeBuild proyek Anda. Untuk informasi selengkapnya, lihat Menggunakan AWS Config dengan CodeBuild sampel di Panduan AWS CodeBuild Pengguna.

AWS X-Ray

AWS X-Ray terintegrasi dengan AWS Config untuk merekam perubahan konfigurasi yang dibuat pada sumber daya enkripsi X-Ray Anda. Anda dapat menggunakan AWS Config inventaris sumber daya enkripsi X-Ray, mengaudit riwayat konfigurasi X-Ray, dan mengirim pemberitahuan berdasarkan perubahan sumber daya. Untuk informasi selengkapnya, lihat Melacak perubahan konfigurasi enkripsi X-Ray AWS Config di Panduan AWS X-Ray Pengembang.

AWS Service Management Connector

The AWS Service Management Connector for ServiceNow dapat menyinkronkan AWS Config data dari beberapa akun dan Wilayah menggunakan Aggregator. Untuk informasi selengkapnya, lihat Mengintegrasikan AWS Config ServiceNow dalam Panduan AWS Service Management Connector Administrator.

Amazon API Gateway

Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi yang dibuat pada resource API Gateway API dan mengirim notifikasi berdasarkan perubahan sumber daya. Mempertahankan riwayat perubahan konfigurasi untuk sumber daya API Gateway berguna untuk pemecahan masalah operasional, audit, dan kasus penggunaan kepatuhan. Untuk informasi selengkapnya, lihat Memantau konfigurasi API Gateway API dengan AWS Config Panduan Pengembang API Gateway.

Region Support untuk AWS Config

Pertimbangan

Beberapa fitur hanya AWS Config didukung dalam subset AWS Wilayah di mana AWS Config didukung.

Manajemen Sumber Daya

- Untuk daftar jenis AWS sumber daya yang didukung di Wilayah mana, lihat Cakupan Sumber Daya menurut Ketersediaan Wilayah.

AWS Config Aturan

- Untuk daftar AWS Config aturan yang didukung di Wilayah mana, lihat Daftar Aturan AWS Config Terkelola menurut Ketersediaan Wilayah.
- Untuk daftar Wilayah yang mendukung penerapan aturan organisasi, lihat AWS Config Aturan Organisasi | Dukungan Wilayah.

Paket Kesesuaian

- Untuk daftar Wilayah yang mendukung paket kesesuaian dan penerapan organisasi paket kesesuaian, lihat Paket Kesesuaian | Dukungan Wilayah.

Remediasi

- Untuk daftar Wilayah yang mendukung tindakan remediasi untuk AWS Config aturan, lihat Tindakan Remediasi | Dukungan Wilayah.

Agregator

- Untuk daftar Wilayah yang mendukung agregator, lihat Agregator | Dukungan Wilayah.

Pertanyaan Lanjutan

- Untuk daftar Wilayah yang mendukung kueri lanjutan, lihat Kueri Lanjutan | Dukungan Wilayah.

- Untuk daftar Wilayah yang mendukung pemroses kueri bahasa alami untuk kueri lanjutan, lihat Pemroses kueri bahasa alami untuk kueri lanjutan | Dukungan Wilayah.

Daftar Wilayah yang Didukung

Tabel berikut mencantumkan AWS Wilayah tempat Anda dapat mengaktifkan AWS Config.

Nama Wilayah	Wilayah	Titik Akhir	Protokol
AS Timur (Ohio)	us–east-2	config.us-east-2.amazonaws.com config-fips.us-east-2.amazonaws.com	HTTPS HTTPS
AS Timur (Virginia Utara)	us-east-1	config.us-east-1.amazonaws.com config-fips.us-east-1.amazonaws.com	HTTPS HTTPS
AS Barat (Californ ia Utara)	us-west-1	config.us-west-1.amazonaws.com config-fips.us-west-1.amazonaws.com	HTTPS HTTPS
AS Barat (Oregon)	us-west-2	config.us-west-2.amazonaws.com config-fips.us-west-2.amazonaws.com	HTTPS HTTPS
Afrika (Cape Town)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asia Pasifik (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asia Pasifik (Hyderaba d)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Asia Pasifik (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asia Pasifik (Malaysia)	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS
Asia Pasifik (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia Pasifik (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pasifik (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia Pasifik (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia Pasifik (Singapura)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pasifik (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Asia Pasifik (Taipei)	ap-timur-2	config.ap-east-2.amazonaws.com	HTTPS
Asia Pasifik (Thailand)	ap-tenggara 7	config.ap-southeast-7.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Kanada (Pusat)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Kanada Barat (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Eropa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Eropa (Irlandia)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Eropa (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Eropa (Milan)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Eropa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Eropa (Spanyol)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Eropa (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Eropa (Zürich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Meksiko (Tengah)	mx-pusat-1	config.mx-central-1.amazonaws.com	HTTPS
Timur Tengah (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Timur Tengah (UAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
Amerika Selatan (Sao Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (AS-Timur)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol	
AWS GovCloud (AS-Barat)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS	

Batas Layanan untuk AWS Config

Tabel berikut menjelaskan batas dalam AWS Config. Kecuali disebutkan lain, kuota dapat ditingkatkan berdasarkan permintaan. Anda dapat meminta penambahan kuota.

Untuk informasi tentang batasan lain di AWS, lihat Batas AWS Layanan.

Tanda sumber daya

Deskripsi	Nilai Batas	Dapat ditingkatkan
Jumlah maksimum tanda per sumber daya	50	Tidak

AWS Config aturan

Deskripsi	Nilai Batas	Dapat ditingkatkan
Jumlah maksimum AWS Config Aturan per Wilayah per akun	1000	Tidak

Paket Kesesuaian Akun Tunggal

Deskripsi	Nilai Batas	Dapat ditingkatkan
Jumlah maksimum paket kesesuaian per akun	50	Tidak

Deskripsi	Nilai Batas	Dapat ditingkatkan
Jumlah maksimum AWS Config Aturan per paket kesesuaian	130	Tidak

> **Note**
>
> AWS Config aturan dalam paket kesesuaian dihitung dalam batas untuk jumlah maksimum AWS Config Aturan per Wilayah per akun.

Paket Kesesuaian Organisasi

Deskripsi	Nilai Batas	Dapat ditingkatkan
Jumlah maksimum paket kesesuaian per organisasi	50	Tidak
Jumlah maksimum AWS Config Aturan per paket kesesuaian organisasi	130	Tidak

> **Note**
>
> Menerapkan di tingkat organisasi dihitung dalam batas untuk akun anak. AWS Config aturan dalam paket kesesuaian dihitung dalam batas untuk jumlah maksimum AWS Config Aturan per Wilayah per akun.

Agregator

Deskripsi	Nilai Batas	Dapat ditingkatkan
Jumlah maksimum agregator konfigurasi	50	Ya

Deskripsi	Nilai Batas	Dapat ditingkatkan
Jumlah maksimum akun dalam agregator	10000	Tidak
Jumlah maksimum akun yang ditambahkan atau dihapus per minggu untuk semua agregator	1000	Ya

> **Note**
>
> Agregator tingkat organisasi dan agregator akun individu keduanya dihitung dalam batas untuk jumlah maksimum agregator konfigurasi.

Kueri lanjutan

Deskripsi	Nilai Batas	Dapat ditingkatkan
Jumlah maksimum kueri yang disimpan dalam satu akun dan Wilayah	300	Ya

Informasi Tambahan dan Sumber Daya Terkait untuk AWS Config

Sumber daya terkait berikut dapat membantu Anda ketika bekerja dengan layanan ini.

- AWS Config— Halaman web utama untuk informasi tentang AWS Config.
- Penetapan Harga AWS Config
- FAQ Teknis
- AWS Config Rule Development Kit (RDK) — Alat sumber terbuka yang membantu Anda mengatur AWS Config, membuat aturan, dan kemudian mengujinya menggunakan berbagai jenis AWS sumber daya.

- Mitra — Tautan ke produk mitra yang terintegrasi penuh AWS Config untuk membantu Anda memvisualisasikan, memantau, dan mengelola data dari aliran konfigurasi, snapshot konfigurasi, atau riwayat konfigurasi Anda.

- Kelas & Lokakarya - Tautan ke kursus berbasis peran dan khusus, selain laboratorium mandiri untuk membantu mempertajam keterampilan Anda AWS dan mendapatkan pengalaman praktis.
- AWS Pusat Pengembang — Jelajahi tutorial, unduh alat, dan pelajari tentang acara AWS pengembang.
- AWS Alat Pengembang — Tautan ke alat pengembang SDKs, toolkit IDE, dan alat baris perintah untuk mengembangkan dan mengelola AWS aplikasi.
- Memulai Pusat Sumber Daya — Pelajari cara menyiapkan Akun AWS, bergabung dengan AWS komunitas, dan meluncurkan aplikasi pertama Anda.
- Hands-On Tutorial - Ikuti step-by-step tutorial untuk meluncurkan aplikasi pertama Anda. AWS
- AWS Whitepaper — Tautan ke daftar lengkap AWS whitepaper teknis, yang mencakup topik-topik seperti arsitektur, keamanan, dan ekonomi dan ditulis oleh AWS Solutions Architects atau pakar teknis lainnya.
- AWS Dukungan Pusat — Hub untuk membuat dan mengelola AWS Dukungan kasus Anda. Juga termasuk tautan ke sumber daya bermanfaat lainnya, seperti forum, teknis FAQs, status kesehatan layanan, dan AWS Trusted Advisor.
- Dukungan— Halaman web utama untuk informasi tentang Dukungan, saluran dukungan respons cepat untuk membantu Anda membangun dan menjalankan aplikasi di cloud. one-on-one
- Hubungi Kami – Titik kontak pusat untuk pertanyaan tentang tandaihan AWS , akun, peristiwa, penyalahgunaan, dan masalah lainnya.
- AWS Ketentuan Situs — Informasi terperinci tentang hak cipta dan merek dagang kami; akun, lisensi, dan akses situs Anda; dan topik lainnya.

AWS Kit Pengembangan Perangkat Lunak untuk AWS Config

AWS Perangkat pengembangan perangkat lunak (SDK) memudahkan pembuatan aplikasi yang mengakses layanan infrastruktur yang hemat biaya, terukur, dan andal. AWS Dengan AWS SDKs, Anda dapat memulai dalam hitungan menit dengan satu paket yang dapat diunduh yang mencakup perpustakaan, contoh kode, dan dokumentasi referensi. Tabel berikut mencantumkan pustaka yang tersedia SDKs dan pustaka pihak ketiga yang dapat Anda gunakan untuk mengakses secara AWS Config terprogram.

Jenis Akses	Deskripsi
AWS SDKs	AWS menyediakan yang berikut SDKs: • AWS Dokumentasi SDK for C++ • AWS Mobile SDK for iOS Dokumentasi • AWS Dokumentasi SDK for Go • AWS SDK untuk Java Dokumentasi • AWS SDK untuk JavaScript Dokumentasi • AWS SDK untuk .NET Dokumentasi • AWS SDK untuk PHP Dokumentasi • AWS SDK for Python (Boto) Dokumentasi • AWS SDK untuk Ruby Dokumentasi
Perpustakaan pihak ketiga	Pengembang di komunitas AWS pengembang juga menyediakan perpustakaan mereka sendiri, yang dapat Anda temukan di pusat AWS pengembang berikut: • AWS Pusat Pengembang Java • Pusat Pengembang AWS JavaScript • AWS Pusat Pengembang PHP • AWS Pusat Pengembang Python • AWS Pusat Pengembang Ruby • AWS Pusat Pengembang Windows dan .NET

Memulai dengan AWS Config

AWS Config memberikan tampilan rinci tentang konfigurasi AWS sumber daya di Anda Akun AWS. Dengan AWS Config, Anda dapat meninjau perubahan konfigurasi dan hubungan antar AWS sumber daya, menjelajahi riwayat konfigurasi sumber daya, dan menggunakan aturan untuk menentukan kepatuhan. Untuk informasi lebih lanjut, lihat Apa itu AWS Config? dan bagaimana cara AWS Config kerjanya.

Mendaftar untuk AWS

Topik

- Mendaftar untuk Akun AWS
- Buat pengguna dengan akses administratif

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/pendaftaran.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan menerima panggilan telepon atau pesan teks dan memasukkan kode verifikasi pada keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS mengirimkan email konfirmasi setelah proses pendaftaran selesai. Kapan saja, Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan masuk https://aws.amazon.comke/ dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

   Untuk bantuan masuk dengan menggunakan pengguna root, lihat Masuk sebagai pengguna root di AWS Sign-In Panduan Pengguna.

2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

   Untuk petunjuk, lihat Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root (konsol) Anda di Panduan Pengguna IAM.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

   Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .

2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

   Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email saat Anda membuat pengguna Pusat Identitas IAM.

  Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat Masuk ke portal AWS akses di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat Identitas IAM, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

   Untuk petunjuk, lihat Membuat set izin di Panduan AWS IAM Identity Center Pengguna.
2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

   Untuk petunjuk, lihat Menambahkan grup di Panduan AWS IAM Identity Center Pengguna.

Cara Memulai dengan AWS Config

Setelah Anda mendaftar untuk Akun AWS, Anda dapat memulai AWS Config dengan AWS Management Console, AWS CLI, atau. AWS SDKs

- Menyiapkan AWS Config dengan Konsol
- Menyiapkan AWS Config dengan AWS CLI
- Menggunakan AWS Config layanan dengan AWS SDK

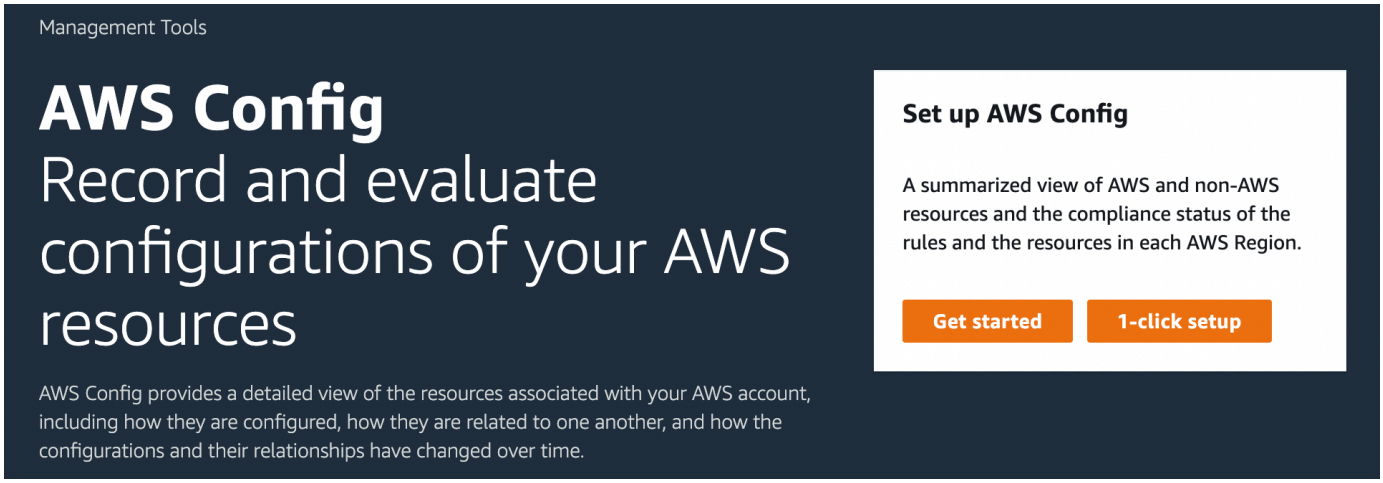
Menyiapkan AWS Config dengan Konsol

AWS Management Console Ini menyediakan proses yang cepat dan efisien untuk pengaturan AWS Config.

Pengaturan

Untuk mengatur AWS Config dengan konsol

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Jika ini adalah pertama kalinya Anda membuka AWS Config konsol atau Anda menyiapkan AWS Config di wilayah baru, halaman AWS Config konsol terlihat seperti berikut:



3. Pilih pengaturan 1-klik untuk diluncurkan AWS Config berdasarkan praktik AWS terbaik. Anda juga dapat memilih Mulai untuk melalui proses pengaturan yang lebih rinci.

Topik

- Pengaturan 1-klik untuk AWS Config
- Pengaturan manual untuk AWS Config

Pengaturan 1-klik untuk AWS Config

AWS Config Pengaturan 1-klik membantu menyederhanakan proses memulai untuk pelanggan AWS Config konsol dengan mengurangi jumlah pilihan manual. Untuk menelusuri semua pilihan manual dari proses penyiapan, lihat Pengaturan manual.

Untuk mengatur AWS Config dengan konsol menggunakan pengaturan 1-klik

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Pilih pengaturan 1-klik.

Halaman pengaturan mencakup tiga langkah, tetapi melalui alur kerja pengaturan 1-klik, Anda secara otomatis diarahkan ke Langkah 3 (Tinjauan). Berikut ini memberikan rincian prosedur itu.

- Pengaturan: Untuk memilih cara AWS Config konsol merekam sumber daya dan peran, dan memilih di mana riwayat konfigurasi dan file snapshot konfigurasi dikirim.

- Aturan: Untuk AWS Config aturan dukungan Wilayah AWS itu, langkah ini tersedia bagi Anda untuk mengonfigurasi aturan terkelola awal yang dapat Anda tambahkan ke akun Anda. Setelah menyiapkan, AWS Config akan mengevaluasi AWS sumber daya Anda terhadap aturan yang Anda pilih. Aturan tambahan dapat dibuat dan yang sudah ada dapat diperbarui di akun Anda setelah penyiapan.
- Ulasan: Untuk memverifikasi detail penyiapan Anda.

Langkah 1: Pengaturan

Strategi perekaman

Opsi untuk merekam Semua jenis sumber daya dengan penggantian yang dapat disesuaikan dipilih untuk Anda. AWS Config akan merekam semua jenis sumber daya yang didukung saat ini dan masa depan di Wilayah ini. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.

- Pengaturan default

  Frekuensi perekaman default diatur ke Continuous untuk Anda. Ini berarti AWS Config mencatat perubahan konfigurasi terus menerus setiap kali terjadi perubahan.

  AWS Config juga mendukung opsi untuk mengatur frekuensi perekaman ke Harian. Jika Anda memilih opsi ini setelah penyiapan, Anda akan menerima item konfigurasi (CI) yang mewakili status terbaru sumber daya Anda selama periode 24 jam terakhir, hanya jika berbeda dari CI sebelumnya yang direkam. Untuk informasi lebih lanjut lihat, Frekuensi Perekaman.

  > **Note**
  >
  > AWS Firewall Manager tergantung pada perekaman berkelanjutan untuk memantau sumber daya Anda. Jika Anda menggunakan Firewall Manager, disarankan agar Anda mengatur frekuensi perekaman ke Continuous.

- Mengganti pengaturan - opsional

  Secara opsional, setelah penyiapan, Anda dapat mengganti frekuensi rekaman untuk jenis sumber daya tertentu, atau mengecualikan jenis sumber daya tertentu dari perekaman. Untuk mengganti pengaturan default, pilih Pengaturan di navigasi kiri AWS Config konsol, lalu pilih Edit.

Pertimbangan Saat Merekam Sumber Daya

Jumlah AWS Config Evaluasi yang Tinggi

Anda mungkin melihat peningkatan aktivitas di akun selama perekaman bulan awal dengan AWS Config jika dibandingkan dengan bulan-bulan berikutnya. Selama proses bootstrap awal, AWS Config jalankan evaluasi pada semua sumber daya di akun Anda yang telah Anda pilih untuk direkam. AWS Config

Jika Anda menjalankan beban kerja sementara, Anda mungkin melihat peningkatan aktivitas dari AWS Config saat merekam perubahan konfigurasi yang terkait dengan pembuatan dan penghapusan sumber daya sementara ini. Beban kerja sementara adalah penggunaan sementara sumber daya komputasi yang dimuat dan dijalankan saat diperlukan. Contohnya termasuk Instans Spot Amazon Elastic Compute Cloud (Amazon EC2), pekerjaan EMR Amazon, dan. AWS Auto Scaling Jika Anda ingin menghindari peningkatan aktivitas menjalankan beban kerja sementara, Anda dapat mengatur perekam konfigurasi untuk mengecualikan jenis sumber daya ini agar tidak direkam, atau menjalankan jenis beban kerja ini di akun terpisah dengan AWS Config dimatikan untuk menghindari peningkatan perekaman konfigurasi dan evaluasi aturan.

Jenis sumber daya global | Kluster global Aurora pada awalnya disertakan dalam rekaman

Jenis `AWS::RDS::GlobalCluster` sumber daya akan direkam di semua AWS Config Wilayah yang didukung tempat perekam konfigurasi diaktifkan.

Jika Anda tidak ingin merekam `AWS::RDS::GlobalCluster` di semua Wilayah yang diaktifkan, Anda dapat mengecualikan jenis sumber daya ini dari perekaman setelah penyiapan. Pilih Pengaturan di bilah navigasi kiri, lalu pilih Edit. Dari Edit, buka Pengaturan ganti di bagian Metode perekaman, pilih`AWS::RDS::GlobalCluster`, dan pilih ganti “Kecualikan dari perekaman”.

Jenis sumber daya global | Jenis sumber daya IAM awalnya dikecualikan dari perekaman

“Semua jenis sumber daya IAM yang direkam secara global” pada awalnya dikecualikan dari pencatatan untuk membantu Anda mengurangi biaya. Paket ini mencakup pengguna IAM, grup, peran, dan kebijakan yang dikelola pelanggan. Pilih Hapus untuk menghapus penggantian dan menyertakan sumber daya ini dalam rekaman Anda.

Selain itu, jenis sumber daya IAM global (`AWS::IAM::User`,`AWS::IAM::Group`,`AWS::IAM::Role`, dan`AWS::IAM::Policy`) tidak dapat dicatat di Wilayah yang didukung AWS Config setelah Februari 2022. Untuk daftar Wilayah tersebut, lihat Merekam AWS Sumber Daya | Sumber Daya Global.

Tata kelola data

Periode penyimpanan data default untuk menyimpan AWS Config data selama 7 tahun (2557 hari) dipilih untuk Anda di bagian ini.

Opsi untuk Menggunakan peran AWS Config terkait layanan yang ada dipilih untuk Anda dan disetel ke peran.AWS Config Peran terkait layanan telah ditentukan sebelumnya oleh AWS Config dan menyertakan semua izin yang diperlukan layanan untuk memanggil layanan lain. AWS

Metode pengiriman

Opsi untuk Memilih ember dari akun Anda dipilih untuk Anda di bagian ini. Pilihan ini akan default ke bucket di akun Anda yang diberi nama dalam format`config-bucket-`*`accountid`*. Misalnya, `config-bucket-012345678901`. Jika Anda tidak memiliki ember yang dibuat dalam format itu, satu akan dibuat untuk Anda. Jika Anda ingin membuat bucket sendiri, lihat Membuat bucket di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Untuk informasi selengkapnya tentang bucket S3, lihat ikhtisar Bucket di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Langkah 2: Aturan

Di bawah Aturan AWS Terkelola, tidak ada aturan yang dipilih untuk Anda pada langkah ini. Sebagai gantinya, Anda dianjurkan untuk membuat dan memperbarui aturan setelah Anda selesai menyiapkan akun Anda.

Langkah 3: Tinjau

Tinjau detail AWS Config penyiapan Anda. Anda dapat kembali untuk mengedit perubahan untuk setiap bagian. Pilih Konfirmasi untuk menyelesaikan pengaturan AWS Config.

Pengaturan manual untuk AWS Config

Dengan alur kerja Memulai, Anda dapat melalui semua pilihan manual dari proses penyiapan untuk memulai dengan konsol. AWS Config Untuk proses memulai yang disederhanakan, lihat Pengaturan 1-klik.

Untuk mengatur AWS Config dengan konsol menggunakan Memulai

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.

2. Pilih Mulai.

Halaman pengaturan mencakup tiga langkah. Berikut ini memberikan rincian prosedur itu setelah Anda memilih Memulai.

- Pengaturan: Untuk memilih cara AWS Config konsol merekam sumber daya dan peran, dan memilih di mana riwayat konfigurasi dan file snapshot konfigurasi dikirim.
- Aturan: Untuk AWS Config aturan dukungan Wilayah AWS itu, langkah ini tersedia bagi Anda untuk mengonfigurasi aturan terkelola awal yang dapat Anda tambahkan ke akun Anda. Setelah menyiapkan, AWS Config akan mengevaluasi AWS sumber daya Anda terhadap aturan yang Anda pilih. Aturan tambahan dapat dibuat dan yang sudah ada dapat diperbarui dan di akun Anda setelah penyiapan.
- Ulasan: Untuk memverifikasi detail penyiapan Anda.

Langkah 1: Pengaturan

Strategi perekaman

Di bagian Metode perekaman, pilih strategi perekaman. Anda dapat menentukan AWS sumber daya yang AWS Config ingin Anda rekam.

All resource types with customizable overrides

Siapkan AWS Config untuk merekam perubahan konfigurasi untuk semua jenis sumber daya yang didukung saat ini dan masa depan di Wilayah ini. Anda dapat mengganti frekuensi perekaman untuk jenis sumber daya tertentu atau mengecualikan jenis sumber daya tertentu dari perekaman. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.

- Pengaturan default

  Konfigurasikan frekuensi perekaman default untuk semua jenis sumber daya yang didukung saat ini dan masa depan. Untuk informasi lebih lanjut lihat, Frekuensi Perekaman.

  - Perekaman berkelanjutan - AWS Config akan merekam perubahan konfigurasi secara terus menerus setiap kali terjadi perubahan.
  - Rekaman harian — Anda akan menerima item konfigurasi (CI) yang mewakili status terbaru sumber daya Anda selama periode 24 jam terakhir, hanya jika berbeda dari CI sebelumnya yang direkam.

> **Note**
>
> AWS Firewall Manager tergantung pada perekaman berkelanjutan untuk memantau sumber daya Anda. Jika Anda menggunakan Firewall Manager, disarankan agar Anda mengatur frekuensi perekaman ke Continuous.

- Ganti pengaturan

  Ganti frekuensi perekaman untuk jenis sumber daya tertentu, atau kecualikan jenis sumber daya tertentu dari perekaman. Jika Anda mengubah frekuensi perekaman untuk jenis sumber daya atau berhenti merekam jenis sumber daya, item konfigurasi yang sudah direkam akan tetap tidak berubah.

Specific resource types

Setel AWS Config untuk merekam perubahan konfigurasi hanya untuk jenis sumber daya yang Anda tentukan.

- Jenis sumber daya tertentu

  Pilih jenis sumber daya untuk merekam dan frekuensinya. Untuk informasi lebih lanjut lihat, Frekuensi Perekaman.

  - Perekaman berkelanjutan - AWS Config akan merekam perubahan konfigurasi secara terus menerus setiap kali terjadi perubahan.
  - Rekaman harian — Anda akan menerima item konfigurasi (CI) yang mewakili status terbaru sumber daya Anda selama periode 24 jam terakhir, hanya jika berbeda dari CI sebelumnya yang direkam.

  > **Note**
  >
  > AWS Firewall Manager tergantung pada perekaman berkelanjutan untuk memantau sumber daya Anda. Jika Anda menggunakan Firewall Manager, disarankan agar Anda mengatur frekuensi perekaman ke Continuous.

  Jika Anda mengubah frekuensi perekaman untuk jenis sumber daya atau berhenti merekam jenis sumber daya, item konfigurasi yang sudah direkam akan tetap tidak berubah.

Pertimbangan Saat Merekam Sumber Daya

Jumlah AWS Config Evaluasi yang Tinggi

Anda mungkin melihat peningkatan aktivitas di akun selama perekaman bulan awal dengan AWS Config jika dibandingkan dengan bulan-bulan berikutnya. Selama proses bootstrap awal, AWS Config jalankan evaluasi pada semua sumber daya di akun Anda yang telah Anda pilih untuk direkam. AWS Config

Jika Anda menjalankan beban kerja sementara, Anda mungkin melihat peningkatan aktivitas dari AWS Config saat merekam perubahan konfigurasi yang terkait dengan pembuatan dan penghapusan sumber daya sementara ini. Beban kerja sementara adalah penggunaan sementara sumber daya komputasi yang dimuat dan dijalankan saat diperlukan. Contohnya termasuk Instans Spot Amazon Elastic Compute Cloud (Amazon EC2), pekerjaan EMR Amazon, dan. AWS Auto Scaling Jika Anda ingin menghindari peningkatan aktivitas menjalankan beban kerja sementara, Anda dapat mengatur perekam konfigurasi untuk mengecualikan jenis sumber daya ini agar tidak direkam, atau menjalankan jenis beban kerja ini di akun terpisah dengan AWS Config dimatikan untuk menghindari peningkatan perekaman konfigurasi dan evaluasi aturan.

Considerations: All resource types with customizable overrides

- Jenis sumber daya yang direkam secara global | Kluster global Aurora pada awalnya disertakan dalam rekaman

  Jenis `AWS::RDS::GlobalCluster` sumber daya akan direkam di semua AWS Config Wilayah yang didukung tempat perekam konfigurasi diaktifkan.

  Jika Anda tidak ingin merekam `AWS::RDS::GlobalCluster` di semua Wilayah yang diaktifkan, pilih "AWS RDS GlobalCluster“, dan pilih penggantian “Kecualikan dari perekaman”.

  Jenis sumber daya global | Jenis sumber daya IAM awalnya dikecualikan dari perekaman

  Jenis sumber daya IAM global pada awalnya dikecualikan dari pencatatan untuk membantu Anda mengurangi biaya. Paket ini mencakup pengguna IAM, grup, peran, dan kebijakan yang dikelola pelanggan. Pilih Hapus untuk menghapus penggantian dan menyertakan sumber daya ini dalam rekaman Anda.

  Selain itu, jenis sumber daya IAM global (`AWS::IAM::User`,`AWS::IAM::Group`,`AWS::IAM::Role`, dan`AWS::IAM::Policy`) tidak dapat dicatat di Wilayah yang didukung AWS Config setelah Februari 2022. Untuk daftar Wilayah tersebut, lihat Merekam AWS Sumber Daya | Sumber Daya Global.

Batas

Anda dapat menambahkan hingga 100 penggantian frekuensi dan 600 penggantian pengecualian.

Rekaman harian tidak dapat ditentukan untuk jenis sumber daya berikut:

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

Considerations: Specific resource types

Ketersediaan Wilayah

Sebelum menentukan jenis sumber daya AWS Config untuk dilacak, periksa Cakupan Sumber Daya menurut Ketersediaan Wilayah untuk melihat apakah jenis sumber daya didukung di AWS Wilayah tempat Anda menyiapkan AWS Config. Jika jenis sumber daya didukung oleh AWS Config setidaknya satu Wilayah, Anda dapat mengaktifkan perekaman jenis sumber daya tersebut di semua Wilayah yang didukung oleh AWS Config, meskipun jenis sumber daya yang ditentukan tidak didukung di AWS Wilayah tempat Anda menyiapkan AWS Config.

Batas

Tidak ada batasan jika semua jenis sumber daya memiliki frekuensi yang sama. Anda dapat menambahkan hingga 100 jenis sumber daya dengan frekuensi Harian jika setidaknya satu jenis sumber daya diatur ke Continuous.

Frekuensi harian tidak didukung untuk jenis sumber daya berikut:

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

Tata kelola data

- Untuk periode penyimpanan data, pilih periode penyimpanan default untuk menyimpan AWS Config data selama 7 tahun (2557) atau tetapkan periode sewa khusus untuk item yang direkam oleh. AWS Config

AWS Config memungkinkan Anda untuk menghapus data Anda dengan menentukan periode retensi untuk Anda`ConfigurationItems`. Saat Anda menentukan periode retensi, AWS Config pertahankan periode Anda `ConfigurationItems` untuk periode yang ditentukan. Anda dapat memilih periode antara minimal 30 hari dan maksimal 7 tahun (2557 hari). AWS Config menghapus data yang lebih lama dari periode retensi yang Anda tentukan.

- Untuk peran IAM AWS Config, pilih peran AWS Config terkait layanan yang ada atau peran IAM dari akun Anda.
  - Peran terkait layanan telah ditentukan sebelumnya oleh AWS Config dan menyertakan semua izin yang diperlukan layanan untuk memanggil layanan lain. AWS

    > **Note**
    >
    > Direkomendasikan: Gunakan peran terkait Layanan
    > Disarankan agar Anda menggunakan peran terkait layanan. Peran terkait layanan menambahkan semua izin yang diperlukan untuk menjalankan seperti yang AWS Config diharapkan.

  - Jika tidak, pilih peran IAM dari salah satu peran dan kebijakan izin Anda yang sudah ada sebelumnya.

    > **Note**
    >
    > Kebijakan dan hasil kepatuhan
    > Kebijakan IAM dan kebijakan lain yang dikelola AWS Organizations dapat memengaruhi apakah AWS Config memiliki izin untuk merekam perubahan konfigurasi untuk sumber daya Anda. Selain itu, aturan secara langsung mengevaluasi konfigurasi sumber daya dan aturan tidak memperhitungkan kebijakan ini saat menjalankan evaluasi. Pastikan bahwa kebijakan yang berlaku selaras dengan cara Anda berniat untuk menggunakan AWS Config.
    > Pertahankan Izin Minimum Saat Menggunakan Kembali peran IAM
    > Jika Anda menggunakan AWS layanan yang menggunakan AWS Config, seperti AWS Security Hub atau AWS Control Tower, dan peran IAM telah dibuat, pastikan bahwa peran IAM yang Anda gunakan saat menyiapkan AWS Config memiliki izin minimum yang sama dengan peran IAM yang sudah ada sebelumnya. Anda harus melakukan ini untuk memastikan bahwa AWS layanan lain terus berjalan seperti yang diharapkan.

Misalnya, jika AWS Control Tower memiliki peran IAM yang memungkinkan AWS Config untuk membaca objek S3, pastikan bahwa izin yang sama diberikan ke peran IAM yang Anda gunakan saat menyiapkan. AWS Config Jika tidak, itu dapat mengganggu cara AWS Control Tower beroperasi.

Metode pengiriman

- Untuk metode Pengiriman, pilih bucket S3 yang akan AWS Config mengirimkan riwayat konfigurasi dan berkas snapshot konfigurasi:
  - Buat bucket — Untuk nama bucket S3, ketikkan nama untuk bucket S3 Anda.

    Nama yang Anda ketik harus unik di semua nama bucket yang ada di Amazon S3. Salah satu cara untuk membantu memastikan keunikan adalah dengan memasukkan awalan; misalnya, nama organisasi Anda. Anda tidak dapat mengubah nama bucket setelah dibuat. Untuk informasi selengkapnya, lihat Pembatasan dan Batasan Bucket di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.
  - Pilih bucket dari akun Anda — Untuk nama bucket S3, pilih bucket pilihan Anda.
  - Pilih bucket dari akun lain — Untuk nama bucket S3, ketikkan nama bucket.

    > **Note**
    >
    > Izin Bucket
    > Jika Anda memilih bucket dari akun lain, bucket tersebut harus memiliki kebijakan yang memberikan izin akses AWS Config. Untuk informasi selengkapnya, lihat Izin untuk Bucket Amazon S3 untuk AWS Config Saluran Pengiriman.
- Untuk topik Amazon SNS, pilih Streaming perubahan konfigurasi dan notifikasi ke topik Amazon SNS agar AWS Config pemberitahuan kirim seperti pengiriman riwayat konfigurasi, pengiriman snapshot konfigurasi, dan kepatuhan.
- Jika Anda memilih untuk melakukan AWS Config streaming ke topik Amazon SNS, pilih topik target:
  - Buat topik - Untuk Nama Topik, ketikkan nama untuk topik SNS Anda.
  - Pilih topik dari akun Anda — Untuk Nama Topik, pilih topik yang Anda inginkan.
  - Pilih topik dari akun lain — Untuk Topik ARN, ketik Nama Sumber Daya Amazon (ARN) dari topik tersebut. Jika Anda memilih topik dari akun lain, topik tersebut harus memiliki kebijakan

yang memberikan izin akses AWS Config. Untuk informasi selengkapnya, lihat Izin untuk Topik Amazon SNS.

> **Note**
>
> Wilayah untuk Topik Amazon SNS
> Topik Amazon SNS harus ada di Wilayah yang sama dengan Wilayah tempat Anda mengatur. AWS Config

Langkah 2: Aturan

Jika Anda menyiapkan AWS Config di Wilayah yang mendukung aturan, pilih Berikutnya.

Langkah 3: Tinjau

Tinjau detail AWS Config penyiapan Anda. Anda dapat kembali untuk mengedit perubahan untuk setiap bagian. Pilih Konfirmasi untuk menyelesaikan pengaturan AWS Config.

Untuk informasi selengkapnya

Untuk informasi tentang mencari sumber daya yang ada di akun Anda dan memahami konfigurasi sumber daya Anda, lihat Mencari Sumber Daya, MelihatInforman Kepatuhan, dan Melihat Riwayat Kepatuhan.

Anda juga dapat menggunakan Amazon Simple Queue Service untuk memantau AWS sumber daya secara terprogram. Lihat informasi yang lebih lengkap di Memantau Perubahan AWS Sumber Daya dengan Amazon SQS.

Menyiapkan AWS Config dengan AWS CLI

AWS CLI Ini adalah alat terpadu untuk mengelola AWS layanan Anda. Dengan hanya satu alat untuk mengunduh dan mengkonfigurasi, Anda dapat mengontrol beberapa AWS layanan dari baris perintah dan menggunakan skrip untuk mengotomatiskannya. Untuk informasi selengkapnya tentang AWS CLI dan untuk petunjuk tentang cara menginstal AWS CLI alat, lihat yang berikut ini di Panduan AWS Command Line Interface Pengguna.

- AWS Command Line Interface Panduan Pengguna
- Mempersiapkan AWS Command Line Interface

Jika perlu, masukkan `aws configure` untuk mengkonfigurasi AWS CLI untuk menggunakan AWS Wilayah di mana AWS Config tersedia.

Pengaturan

Lihat topik berikut untuk disiapkan AWS Config dengan AWS CLI.

Topik

- Prasyarat untuk Menyiapkan dengan AWS ConfigAWS CLI
- Dimulai AWS Config dengan perekam konfigurasi yang dikelola pelanggan menggunakan AWS CLI
- Memverifikasi bahwa Berhasil AWS Config Dimulai dengan AWS CLI

Prasyarat untuk Menyiapkan dengan AWS ConfigAWS CLI

Sebelum menyiapkan AWS AWS CLI, Anda perlu membuat bucket Amazon S3, topik Amazon SNS, dan peran IAM dengan kebijakan terlampir sebagai prasyarat. Anda kemudian dapat menggunakan AWS CLI untuk menentukan bucket, topik, dan peran untuk AWS Config. Ikuti prosedur ini untuk mengatur prasyarat Anda. AWS Config

Topik

- Langkah 1: Membuat Bucket Amazon S3
- Langkah 2: Membuat Topik Amazon SNS
- Langkah 3: Membuat Peran IAM

Langkah 1: Membuat Bucket Amazon S3

Jika Anda sudah memiliki ember Amazon S3 di akun Anda dan ingin menggunakannya, lewati langkah ini dan buka. Langkah 2: Membuat Topik Amazon SNS

Menggunakan konsol S3

Untuk membuat bucket

1. Buka konsol Amazon S3 di. https://console.aws.amazon.com/s3/
2. Pilih Buat bucket.
3. Di Nama bucket, masukkan nama yang sesuai dengan DNS untuk bucket Anda.

Nama kelompok harus:

- Unik di seluruh Amazon S3.
- Panjangnya antara 3 dan 63 karakter.
- Tidak mengandung karakter huruf besar.
- Mulai dengan huruf kecil atau angka.

Setelah membuat bucket, Anda tidak dapat mengubah namanya. Pastikan nama bucket yang Anda pilih unik di semua nama bucket yang ada di Amazon S3. Untuk informasi selengkapnya tentang aturan dan konvensi penamaan bucket, lihat Pembatasan dan Batasan Bucket di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

> **Important**
>
> Hindari memasukkan informasi sensitif ke dalam nama bucket. Nama ember terlihat di titik URLs itu ke objek di ember.

4. Di Wilayah, pilih AWS Wilayah tempat Anda ingin ember berada.

   Pilih Wilayah yang dekat dengan Anda untuk meminimalkan latensi dan biaya serta memenuhi persyaratan regulasi. Objek yang disimpan di Wilayah tidak pernah keluar dari Wilayah kecuali Anda secara tegas mentransfer atau mereplikasinya ke Wilayah lain. Untuk daftar AWS Wilayah Amazon S3, lihat titik akhir AWS layanan di. Referensi Umum Amazon Web Services

5. Pada Pengaturan bucket untuk Blokir Akses Publik, pilih pengaturan Blokir Akses Publik yang ingin Anda terapkan ke bucket.

   Kami menyarankan agar Anda membiarkan semua pengaturan diaktifkan, kecuali jika Anda tahu Anda perlu mematikan satu atau lebih pengaturan tersebut untuk kasus penggunaan Anda, seperti untuk menyelenggarakan situs web publik. Blokir pengaturan akses publik yang Anda aktifkan untuk bucket juga akan diaktifkan untuk semua titik akses yang Anda buat pada bucket. Untuk informasi selengkapnya tentang memblokir akses publik, lihat Menggunakan Amazon S3 Blokir Akses Publik di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

6. (Opsional) Jika Anda ingin mengaktifkan Kunci Objek S3:

   a. Pilih Pengaturan lanjutan, dan baca pesan yang muncul.

> **Important**
>
> Anda hanya dapat mengaktifkan Kunci Objek S3 untuk bucket saat Anda membuatnya. Jika Anda mengaktifkan Kunci Objek untuk bucket, Anda tidak dapat menonaktifkannya nanti. Mengaktifkan Kunci Objek juga memungkinkan pembuatan versi untuk bucket. Setelah Anda mengaktifkan Kunci Objek untuk bucket, Anda harus mengonfigurasi pengaturan Kunci Objek sebelum objek apa pun dalam bucket dilindungi. Untuk informasi selengkapnya tentang mengonfigurasi perlindungan untuk objek, lihat Mengonfigurasi Kunci Objek S3 menggunakan konsol Amazon S3.

b. Jika Anda ingin mengaktifkan Kunci Objek, masukkan aktifkan di kotak teks dan memilih Konfirmasi.

Untuk informasi selengkapnya tentang fitur Kunci Objek S3, lihat Mengunci Objek Menggunakan Kunci Objek Amazon S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

7. Pilih Buat bucket.

Menggunakan AWS SDKs

Bila Anda menggunakan AWS SDKs untuk membuat bucket, Anda harus membuat klien dan kemudian menggunakan klien untuk mengirim permintaan untuk membuat bucket. Sebagai praktik terbaik, Anda harus membuat klien dan bucket di Wilayah AWS yang sama. Jika Anda tidak menentukan Wilayah saat membuat klien atau bucket, Amazon S3 menggunakan Wilayah default US East (N. Virginia).

Untuk membuat klien untuk mengakses titik akhir dual-stack, Anda harus menentukan. Wilayah AWS Untuk informasi selengkapnya, lihat titik akhir tumpukan ganda Amazon S3. Untuk daftar yang tersedia Wilayah AWS, lihat Wilayah dan titik akhir di. Referensi Umum AWS

Saat Anda membuat klien, Wilayah akan memetakan ke titik akhir spesifik Wilayah. Klien menggunakan titik akhir ini untuk berkomunikasi dengan Amazon S3: `s3.<region>.amazonaws.com`. Jika Wilayah Anda diluncurkan setelah 20 Maret 2019, klien dan bucket Anda harus berada di dalam Wilayah yang sama. Namun, Anda dapat menggunakan klien di Wilayah AS Timur (Virginia Utara) untuk membuat bucket di setiap Wilayah yang diluncurkan sebelum 20 Maret 2019. Untuk informasi selengkapnya, lihat Titik Akhir Legacy.

Contoh kode AWS SDK ini melakukan tugas-tugas berikut:

- Membuat klien dengan secara eksplisit menentukan Wilayah AWS — Dalam contoh, klien menggunakan titik akhir `s3.us-west-2.amazonaws.com` untuk berkomunikasi dengan Amazon S3. Anda dapat menentukan Wilayah AWS. Untuk daftar Wilayah AWS, lihat Wilayah dan titik akhir dalam Referensi AWS Umum.
- Kirim permintaan buat bucket dengan hanya menentukan nama bucket — Klien mengirimkan permintaan ke Amazon S3 untuk membuat bucket di Wilayah tempat Anda membuat klien.
- Ambil informasi tentang lokasi bucket — Amazon S3 menyimpan informasi lokasi bucket di subsumber daya lokasi yang dikaitkan dengan bucket.

Contoh kode berikut menunjukkan cara menggunakan`CreateBucket`.

.NET

SDK untuk .NET

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

```
        /// <summary>
        /// Shows how to create a new Amazon S3 bucket.
        /// </summary>
        /// <param name="client">An initialized Amazon S3 client object.</param>
        /// <param name="bucketName">The name of the bucket to create.</param>
        /// <returns>A boolean value representing the success or failure of
        /// the bucket creation process.</returns>
        public static async Task<bool> CreateBucketAsync(IAmazonS3 client, string
bucketName)
        {
            try
            {
                var request = new PutBucketRequest
                {
                    BucketName = bucketName,
                    UseClientRegion = true,
                };
```

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

Buat ember dengan kunci objek diaktifkan.

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

            var response = await _amazonS3.PutBucketAsync(request);

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

```
        }
    }
```

- Untuk detail API, lihat CreateBucketdi Referensi AWS SDK untuk .NET API.

Bash

AWS CLI dengan skrip Bash

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

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

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

###############################################################################
# function create-bucket
#
# This function creates the specified bucket in the specified AWS Region, unless
# it already exists.
```

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

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

  # Retrieve the calling parameters.
  while getopts "b:r:h" option; do
    case "${option}" in
      b) bucket_name="${OPTARG}" ;;
      r) region_code="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
```

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

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

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

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

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

  # shellcheck disable=SC2181
  if [[ ${?} -ne 0 ]]; then
    errecho "ERROR: AWS reports create-bucket operation failed.\n$response"
    return 1
  fi
}
```

- Untuk detail API, lihat CreateBucketdi Referensi AWS CLI Perintah.

C++

SDK untuk C++

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

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

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

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

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

    return outcome.IsSuccess();
}
```

- Untuk detail API, lihat CreateBucketdi Referensi AWS SDK untuk C++ API.

CLI

AWS CLI

Contoh 1: Untuk membuat ember

`create-bucket`Contoh berikut membuat bucket bernama`amzn-s3-demo-bucket`:

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

Output:

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

Lihat informasi yang lebih lengkap di Membuat bucket dalam Panduan Pengguna Amazon S3.

Contoh 2: Untuk membuat ember dengan pemilik diberlakukan

`create-bucket`Contoh berikut membuat bucket bernama yang menggunakan setelan `amzn-s3-demo-bucket` yang diterapkan pemilik bucket untuk Kepemilikan Objek S3.

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

Output:

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

Untuk informasi selengkapnya, lihat Mengontrol kepemilikan objek dan menonaktifkan ACLs di Panduan Pengguna Amazon S3.

Contoh 3: Untuk membuat bucket di luar wilayah ``us-east-1``

`create-bucket`Contoh berikut membuat bucket bernama `amzn-s3-demo-bucket` di `eu-west-1` wilayah tersebut. Daerah di luar `us-east-1` memerlukan yang sesuai `LocationConstraint` untuk ditentukan untuk membuat ember di wilayah yang diinginkan.

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

Output:

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

Lihat informasi yang lebih lengkap di Membuat bucket dalam Panduan Pengguna Amazon S3.

- Untuk detail API, lihat CreateBucketdi Referensi AWS CLI Perintah.

Go

SDK untuk Go V2

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

Buat bucket dengan konfigurasi default.

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

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

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



// CreateBucket creates a bucket with the specified name in the specified Region.
func (basics BucketBasics) CreateBucket(ctx context.Context, name string, region
 string) error {
 _, err := basics.S3Client.CreateBucket(ctx, &s3.CreateBucketInput{
  Bucket: aws.String(name),
  CreateBucketConfiguration: &types.CreateBucketConfiguration{
   LocationConstraint: types.BucketLocationConstraint(region),
  },
 })
 if err != nil {
  var owned *types.BucketAlreadyOwnedByYou
  var exists *types.BucketAlreadyExists
  if errors.As(err, &owned) {
   log.Printf("You already own bucket %s.\n", name)
   err = owned
  } else if errors.As(err, &exists) {
   log.Printf("Bucket %s already exists.\n", name)
   err = exists
  }
 } else {
  err = s3.NewBucketExistsWaiter(basics.S3Client).Wait(
   ctx, &s3.HeadBucketInput{Bucket: aws.String(name)}, time.Minute)
  if err != nil {
   log.Printf("Failed attempt to wait for bucket %s to exist.\n", name)
```

```
  }
 }
 return err
}
```

Buat ember dengan penguncian objek dan tunggu sampai ada.

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

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

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



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

```
 }

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

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

 return bucket, err
}
```

- Untuk detail API, lihat CreateBucketdi Referensi AWS SDK untuk Go API.

Java

SDK untuk Java 2.x

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

Buat bucket.

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

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

           CompletableFuture<WaiterResponse<HeadBucketResponse>>
waiterResponseFuture =
               s3Waiter.waitUntilBucketExists(bucketRequestWait);
           return waiterResponseFuture.thenAccept(waiterResponse -> {
               waiterResponse.matched().response().ifPresent(headBucketResponse
-> {
                   logger.info(bucketName + " is ready");
               });
           });
       }).whenComplete((resp, ex) -> {
           if (ex != null) {
               throw new RuntimeException("Failed to create bucket", ex);
           }
       });
   }
```

Buat ember dengan kunci objek diaktifkan.

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

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

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

- Untuk detail API, lihat CreateBucketdi Referensi AWS SDK for Java 2.x API.

JavaScript

SDK untuk JavaScript (v3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

Buat bucket.

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

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

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

- Untuk informasi selengkapnya, lihat AWS SDK untuk JavaScript Panduan Developer.

- Untuk detail API, lihat CreateBucketdi Referensi AWS SDK untuk JavaScript API.

Kotlin

SDK untuk Kotlin

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

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

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

- Untuk detail API, lihat CreateBucketdi AWS SDK untuk referensi API Kotlin.

PHP

SDK untuk PHP

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

Buat bucket.

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

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

- Untuk detail API, lihat CreateBucketdi Referensi AWS SDK untuk PHP API.

Python

SDK untuk Python (Boto3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

Buat bucket dengan pengaturan default.

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

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


    def create(self, region_override=None):
```

```
        """
        Create an Amazon S3 bucket in the default Region for the account or in
 the
        specified Region.

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

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

Buat bucket berversi dengan konfigurasi siklus hidup.

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

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

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

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

    try:
        bucket.Versioning().enable()
        logger.info("Enabled versioning on bucket %s.", bucket.name)
    except ClientError:
        logger.exception("Couldn't enable versioning on bucket %s.", bucket.name)
        raise

    try:
        expiration = 7
        bucket.LifecycleConfiguration().put(
            LifecycleConfiguration={
                "Rules": [
                    {
                        "Status": "Enabled",
                        "Prefix": prefix,
                        "NoncurrentVersionExpiration": {"NoncurrentDays":
expiration},
                    }
                ]
```

```
            }
        )
        logger.info(
            "Configured lifecycle to expire noncurrent versions after %s days "
            "on bucket %s.",
            expiration,
            bucket.name,
        )
    except ClientError as error:
        logger.warning(
            "Couldn't configure lifecycle on bucket %s because %s. "
            "Continuing anyway.",
            bucket.name,
            error,
        )

    return bucket
```

- Untuk detail API, lihat CreateBucketdi AWS SDK for Python (Boto3) Referensi API.

Ruby

SDK untuk Ruby

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

```
require 'aws-sdk-s3'

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

  # @param bucket [Aws::S3::Bucket] An Amazon S3 bucket initialized with a name.
 This is a client-side object until
  #                                 create is called.
```

```
  def initialize(bucket)
    @bucket = bucket
  end

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

  # Gets the Region where the bucket is located.
  #
  # @return [String] The location of the bucket.
  def location
    if @bucket.nil?
      'None. You must create a bucket before you can get its location!'
    else
      @bucket.client.get_bucket_location(bucket:
 @bucket.name).location_constraint
    end
  rescue Aws::Errors::ServiceError => e
    "Couldn't get the location of #{@bucket.name}. Here's why: #{e.message}"
  end
end

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

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

run_demo if $PROGRAM_NAME == __FILE__
```

- Untuk detail API, lihat CreateBucketdi Referensi AWS SDK untuk Ruby API.

Rust

SDK untuk Rust

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

```
pub async fn create_bucket(
    client: &aws_sdk_s3::Client,
    bucket_name: &str,
    region: &aws_config::Region,
) -> Result<Option<aws_sdk_s3::operation::create_bucket::CreateBucketOutput>,
 S3ExampleError> {
    let constraint =
 aws_sdk_s3::types::BucketLocationConstraint::from(region.to_string().as_str());
    let cfg = aws_sdk_s3::types::CreateBucketConfiguration::builder()
        .location_constraint(constraint)
        .build();
    let create = client
        .create_bucket()
        .create_bucket_configuration(cfg)
        .bucket(bucket_name)
        .send()
        .await;

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

```
        } else {
            Err(S3ExampleError::from(err))
        }
    })
}
```

- Untuk detail API, lihat CreateBucketreferensi AWS SDK for Rust API.

SAP ABAP

SDK untuk SAP ABAP

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

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

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

- Untuk detail API, lihat CreateBucketdi AWS SDK untuk referensi SAP ABAP API.

Swift

SDK untuk Swift

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

```
import AWSS3

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

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

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

```
        catch {
            print("ERROR: ", dump(error, name: "Creating a bucket"))
            throw error
        }
    }
```

- Untuk detail API, lihat referensi CreateBucket AWSSDK untuk Swift API.

> **Note**
>
> Anda juga dapat menggunakan bucket Amazon S3 dari akun lain, tetapi Anda mungkin perlu membuat kebijakan untuk bucket yang memberikan izin akses. AWS Config Untuk informasi tentang pemberian izin ke bucket Amazon S3, Izin untuk Bucket Amazon S3 untuk AWS Config Saluran Pengiriman lihat, lalu buka. Langkah 2: Membuat Topik Amazon SNS

Langkah 2: Membuat Topik Amazon SNS

Jika Anda sudah memiliki topik Amazon SNS di akun Anda dan ingin menggunakannya, lewati langkah ini dan buka. Langkah 3: Membuat Peran IAM

Menggunakan konsol SNS

Untuk membuat topik Amazon SNS

1. Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/ v3/home.
2. Lakukan salah satu tindakan berikut:
   - Jika tidak ada topik yang pernah dibuat di bawah Anda Akun AWS sebelumnya, baca deskripsi Amazon SNS di beranda.
   - Jika topik telah dibuat di bawah Akun AWS sebelumnya, pada panel navigasi, pilih Topik.
3. Di halaman Topics (Topik), pilih Create topic (Buat topik).
4. Di halaman Create topic (Buat topik), di bagian Details (Detail), lakukan hal-hal berikut:
   a. Untuk Type (Jenis), pilih jenis topik (Standar atau FIFO).
   b. Masukkan Nama untuk topik. Untuk topik FIFO, tambahkan .fifo di akhir nama.

c. (Opsional) Masukkan Nama tampilan untuk topik.

d. (Opsional) Untuk topik FIFO, Anda dapat memilih deduplikasi pesan berbasis konten untuk mengaktifkan deduplikasi pesan default. Untuk informasi selengkapnya, lihat Deduplikasi pesan untuk topik FIFO.

5. (Opsional) Perluas bagian Encryption (Enkripsi) dan lakukan hal-hal berikut ini. Untuk informasi selengkapnya, lihat Enkripsi diam.

   a. Pilih Enable encryption (Aktifkan enkripsi).

   b. Tentukan kunci utama pelanggan (customer master key/CMK). Untuk informasi selengkapnya, lihat Syarat kunci.

      Untuk setiap jenis CMK, Description (Deskripsi), Account (Akun), dan ARN CMK ditampilkan.

      > **Important**
      >
      > Jika Anda bukan pemilik CMK, atau jika Anda masuk dengan akun yang tidak memiliki izin `kms:ListAliases` dan `kms:DescribeKey`, Anda tidak akan dapat melihat informasi tentang CMK di konsol Amazon SNS.
      > Minta pemilik CMK untuk memberi Anda izin tersebut. Untuk informasi selengkapnya, lihat Izin API AWS KMS : Referensi Tindakan dan Sumber Daya dalam Panduan Developer AWS Key Management Service .

      - CMK AWS terkelola untuk Amazon SNS (Defaultalias/aws/sns) dipilih secara default.

        > **Note**
        >
        > Ingatlah hal-hal berikut ini:
        >
        > - Pertama kali Anda menggunakan AWS Management Console untuk menentukan CMK AWS terkelola untuk Amazon SNS untuk suatu topik AWS KMS , membuat AWS CMK terkelola untuk Amazon SNS.
        > - Atau, saat pertama kali Anda menggunakan `Publish` tindakan pada topik dengan SSE diaktifkan, AWS KMS membuat CMK AWS terkelola untuk Amazon SNS.

- Untuk menggunakan CMK kustom dari Anda Akun AWS, pilih bidang Customer master key (CMK) dan kemudian pilih CMK kustom dari daftar.

> **Note**
>
> Untuk petunjuk cara membuat kustom CMKs, lihat Membuat Kunci di Panduan AWS Key Management Service Pengembang

- Untuk menggunakan ARN CMK khusus dari akun Akun AWS Anda atau dari akun AWS lain, masukkan ke bidang Customer Master Key (CMK).

6. (Opsional) Secara default, hanya pemilik topik yang dapat menerbitkan atau berlangganan topik. Untuk mengkonfigurasi izin akses tambahan, perluas bagian Access policy (Kebijakan akses). Untuk informasi selengkapnya, lihat Manajemen identitas dan akses di Amazon SNS dan Contoh kasus untuk kontrol akses Amazon SNS.

> **Note**
>
> Saat Anda membuat topik menggunakan konsol tersebut, kebijakan default menggunakan kunci syarat `aws:SourceOwner`. Kunci ini sama dengan `aws:SourceAccount`.

7. (Opsional) Untuk mengkonfigurasi bagaimana Amazon SNS mencoba ulang upaya pengiriman pesan yang gagal, perluas bagian Kebijakan pengiriman ulang (HTTP/S). Untuk informasi selengkapnya, lihat percobaan ulang pengiriman pesan Amazon SNS.
8. (Opsional) Untuk mengonfigurasi cara Amazon SNS mencatat pengiriman pesan ke CloudWatch, perluas bagian Pencatatan status pengiriman. Untuk informasi selengkapnya, lihat status pengiriman pesan Amazon SNS.
9. (Opsional) Untuk menambahkan tag metadata ke topik, perluas bagian Tag, masukkan Kunci dan Nilai (opsional) dan pilih Add tag (Tambahkan tag). Untuk informasi selengkapnya, lihat penandaan topik Amazon SNS.
10. Pilih Buat topik.

    Topik dibuat dan ***MyTopic***halaman ditampilkan.

    Nama, ARN (opsional) Nama tampilan topik, dan ID akun AWS Pemilik topik ditampilkan di bagian Detail.
11. Salin topik ARN ke clipboard, misalnya:

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

Untuk berlangganan alamat email ke topik Amazon SNS

1. Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/ v3/home.
2. Di panel navigasi kiri, pilih Subscriptions (Langganan).
3. Di halaman Subscriptions (Langganan), pilih Create subscription (Buat langganan).
4. Di halaman Create subscription (Buat langganan), di bagian Details (Detail), lakukan:
   a. Untuk Topic ARN (ARN topik), pilih Amazon Resource Name (ARN) dari topik.
   b. Untuk Protocol (Protokol), pilih tipe endpoint. Tipe endpoint yang tersedia adalah:
      - HTTP/HTTPS
      - Email/email-JSON
      - Amazon Data Firehose
      - Amazon SQS

        > **Note**
        > Untuk berlangganan Topik SNS FIFO, pilih opsi ini.

      - AWS Lambda
      - Titik akhir aplikasi platform
      - SMS
   c. Untuk Endpoint, masukkan nilai endpoint, seperti alamat email atau ARN antrean Amazon SQS.
   d. Hanya titik akhir Firehose: Untuk ARN peran Langganan, tentukan ARN dari peran IAM yang Anda buat untuk menulis ke aliran pengiriman Firehose. Untuk informasi selengkapnya, lihat Prasyarat untuk berlangganan aliran pengiriman Firehose ke topik Amazon SNS.
   e. (Opsional) Untuk Firehose, Amazon SQS, endpoint HTTP/S , Anda juga dapat mengaktifkan pengiriman pesan mentah. Untuk informasi selengkapnya, lihat pengiriman pesan mentah Amazon SNS.

f. (Opsional) Untuk mengkonfigurasi kebijakan filter, perluas bagian Subscription filter policy (Kebijakan filter langganan). Untuk informasi selengkapnya, lihat kebijakan filter langganan Amazon SNS.

g. (Opsional) Untuk mengonfigurasi antrean surat mati untuk berlanggana, perluas bagian Redrive policy (dead-letter queue) (Kebijakan redrive (antrean surat mati)). Untuk informasi selengkapnya, lihat antrian surat mati Amazon SNS (). DLQs

h. Pilih Create subscription (Buat langganan).

   Konsol tersebut membuat langganan dan membuka halaman Details (Detail) langganan.

Menggunakan AWS SDKs

Untuk menggunakan AWS SDK, Anda harus mengonfigurasinya dengan kredensi Anda. Untuk informasi selengkapnya, lihat File konfigurasi dan kredensial bersama di Panduan Referensi Alat AWS SDKs dan Alat.

Contoh kode berikut menunjukkan cara menggunakan`CreateTopic`.

.NET

SDK untuk .NET

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

Buat topik dengan nama tertentu.

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

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

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

            IAmazonSimpleNotificationService client = new
 AmazonSimpleNotificationServiceClient();

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

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

            var response = await client.CreateTopicAsync(request);

            return response.TopicArn;
        }
    }
```

Buat topik baru dengan nama dan atribut FIFO dan de-duplikasi tertentu.

```
    /// <summary>
    /// Create a new topic with a name and specific FIFO and de-duplication
 attributes.
    /// </summary>
    /// <param name="topicName">The name for the topic.</param>
```

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

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

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

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

- Untuk detail API, lihat CreateTopicdi Referensi AWS SDK untuk .NET API.

C++

SDK untuk C++

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

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

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

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

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

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

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

- Untuk detail API, lihat CreateTopicdi Referensi AWS SDK untuk C++ API.

CLI

AWS CLI

Untuk membuat topik SNS

`create-topic`Contoh berikut membuat topik SNS bernama`my-topic`.

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

Output:

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

Untuk informasi selengkapnya, lihat Menggunakan Antarmuka Baris AWS Perintah dengan Amazon SQS dan Amazon SNS di Panduan Pengguna Antarmuka Baris AWS Perintah.

- Untuk detail API, lihat CreateTopicdi Referensi AWS CLI Perintah.

Go

SDK untuk Go V2

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

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

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

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



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

```
 }

 return topicArn, err
}
```

- Untuk detail API, lihat CreateTopicdi Referensi AWS SDK untuk Go API.

Java

SDK untuk Java 2.x

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

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

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

                Usage:    <topicName>

                Where:
```

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

                """;

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

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

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

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

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

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

- Untuk detail API, lihat CreateTopicdi Referensi AWS SDK for Java 2.x API.

JavaScript

SDK untuk JavaScript (v3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

Buat klien dalam modul terpisah dan ekspor klien tersebut.

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

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

Mengimpor modul SDK dan klien dan memanggil API.

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

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

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

- Untuk informasi selengkapnya, silakan lihat Panduan Developer AWS SDK untuk JavaScript.
- Untuk detail API, lihat CreateTopicdi Referensi AWS SDK untuk JavaScript API.

Kotlin

SDK untuk Kotlin

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

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

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

- Untuk detail API, lihat CreateTopicdi AWS SDK untuk referensi API Kotlin.

PHP

SDK untuk PHP

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

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

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


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

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

$topicname = 'myTopic';

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

- Untuk informasi selengkapnya, silakan lihat Panduan Developer AWS SDK untuk PHP.
- Untuk detail API, lihat CreateTopicdi Referensi AWS SDK untuk PHP API.

Python

SDK untuk Python (Boto3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

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

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


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

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

- Untuk detail API, lihat CreateTopicdi AWS SDK for Python (Boto3) Referensi API.

Ruby

SDK untuk Ruby

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

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

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

# Example usage:
```

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

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

- Untuk informasi selengkapnya, silakan lihat Panduan Developer AWS SDK untuk Ruby.
- Untuk detail API, lihat CreateTopicdi Referensi AWS SDK untuk Ruby API.

Rust

SDK untuk Rust

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

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

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

    Ok(())
}
```

- Untuk detail API, lihat CreateTopicreferensi AWS SDK for Rust API.

SAP ABAP

SDK untuk SAP ABAP

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

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

- Untuk detail API, lihat CreateTopicdi AWS SDK untuk referensi SAP ABAP API.

Swift

SDK untuk Swift

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

```
import AWSSNS

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

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

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

- Untuk detail API, lihat referensi CreateTopic AWSSDK untuk Swift API.

> **Note**
>
> Anda juga dapat menggunakan topik Amazon SNS di akun lain, tetapi jika demikian Anda mungkin perlu membuat kebijakan untuk topik yang memberikan izin akses. AWS Config Untuk informasi tentang pemberian izin ke topik Amazon SNS, Izin untuk Topik Amazon SNS lihat lalu buka. Langkah 3: Membuat Peran IAM

Langkah 3: Membuat Peran IAM

> **Important**
>
> (Disarankan) Gunakan peran AWS Config terkait layanan
> Disarankan untuk menggunakan peran AWS Config terkait layanan:.
> `AWSServiceRoleForConfig` Peran terkait layanan telah ditentukan sebelumnya dan mencakup semua izin yang AWS Config diperlukan untuk memanggil yang lain. Layanan AWS Peran AWS Config terkait layanan diperlukan untuk perekam konfigurasi terkait layanan.
> Untuk informasi selengkapnya, lihat Menggunakan Peran Tertaut Layanan untuk. AWS Config

Menggunakan konsol IAM

Anda dapat menggunakan konsol IAM untuk membuat peran IAM yang memberikan AWS Config izin untuk mengakses bucket Amazon S3, mengakses topik Amazon SNS, dan mendapatkan detail konfigurasi untuk sumber daya yang didukung. AWS Saat Anda menggunakan konsol untuk membuat peran IAM, AWS Config secara otomatis melampirkan izin yang diperlukan ke peran untuk Anda.

> **Note**
>
> Jika Anda telah menggunakan AWS layanan yang menggunakan AWS Config (seperti AWS Security Hub atau AWS Control Tower) dan AWS Config peran telah dibuat, Anda harus memastikan bahwa peran IAM yang Anda gunakan saat menyiapkan AWS Config hak istimewa minimum yang sama dengan AWS Config peran yang telah dibuat agar AWS layanan lain dapat terus berjalan seperti yang diharapkan.
> Misalnya, jika AWS Control Tower memiliki peran IAM yang memungkinkan AWS Config untuk membaca objek Amazon S3, Anda harus menjamin izin yang sama diberikan dalam peran IAM yang Anda gunakan saat menyiapkan. AWS Config Jika tidak, itu dapat mengganggu operasi Menara AWS Kontrol.
> Untuk informasi selengkapnya tentang peran IAM AWS Config, lihat AWS Identity and Access Management.

Untuk membuat peran untuk AWS layanan

1. Masuk ke AWS Management Console dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi konsol IAM, pilih Peran, dan lalu pilih Buat peran.
3. Untuk Pilih entitas tepercaya, pilih AWS layanan.
4. Pilih kasus penggunaan yang Anda inginkan untuk AWS Config: Config - Customizable, Config - Organizations, Config, atau Config - Conformance Packs. Lalu, pilih Selanjutnya.
5. Pada halaman Nama, tinjau, dan buat, tinjau detail tentang peran Anda, dan pilih Buat Peran.

Menggunakan AWS SDKs

Untuk menggunakan AWS SDK, Anda harus mengonfigurasinya dengan kredensi Anda. Untuk informasi selengkapnya, lihat File konfigurasi dan kredensial bersama di Panduan Referensi Alat AWS SDKs dan Alat.

Contoh kode berikut menunjukkan cara menggunakan`CreateRole`.

.NET

SDK untuk .NET

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

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

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

- Untuk detail API, lihat CreateRoledi Referensi AWS SDK untuk .NET API.

Bash

AWS CLI dengan skrip Bash

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

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

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

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

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

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

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

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

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

local error_code=${?}

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

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

  echo "$response"

  return 0
}
```

- Untuk detail API, lihat CreateRoledi Referensi AWS CLI Perintah.

C++

SDK untuk C++

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

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

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

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

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

    return outcome.IsSuccess();
}
```

- Untuk detail API, lihat CreateRoledi Referensi AWS SDK untuk C++ API.

CLI

AWS CLI

Contoh 1: Untuk membuat peran IAM

`create-role`Perintah berikut membuat peran bernama `Test-Role` dan melampirkan kebijakan kepercayaan padanya.

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

Output:

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

Kebijakan kepercayaan didefinisikan sebagai dokumen JSON dalam file test-role-trust-policy.json. (Nama file dan ekstensi tidak memiliki signifikansi.) Kebijakan kepercayaan harus menentukan kepala sekolah.

Untuk melampirkan kebijakan izin ke peran, gunakan `put-role-policy` perintah.

Untuk informasi selengkapnya, lihat Membuat peran IAM di Panduan Pengguna AWS IAM.

Contoh 2: Untuk membuat peran IAM dengan durasi sesi maksimum yang ditentukan

`create-role`Perintah berikut membuat peran bernama `Test-Role` dan menetapkan durasi sesi maksimum 7200 detik (2 jam).

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

Output:

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

Untuk informasi selengkapnya, lihat Memodifikasi durasi sesi maksimum peran (AWS API) di Panduan Pengguna AWS IAM.

Contoh 3: Untuk membuat Peran IAM dengan tag

Perintah berikut membuat Peran IAM `Test-Role` dengan tag. Contoh ini menggunakan flag `--tags` parameter dengan tag berformat JSON berikut:. `'{"Key": "Department",`

`"Value": "Accounting"}' '{"Key": "Location", "Value": "Seattle"}'`

Atau, `--tags` bendera dapat digunakan dengan tag dalam format singkatan:.

`'Key=Department,Value=Accounting Key=Location,Value=Seattle'`

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

Output:

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

```
}
```

Untuk informasi selengkapnya, lihat Menandai peran IAM di Panduan Pengguna AWS IAM.

- Untuk detail API, lihat CreateRoledi Referensi AWS CLI Perintah.

Go

SDK untuk Go V2

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

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

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

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



// CreateRole creates a role that trusts a specified user. The trusted user can
 assume
// the role to acquire its permissions.
// PolicyDocument shows how to work with a policy document as a data structure
 and
// serialize it to JSON by using Go's JSON marshaler.
```

```
func (wrapper RoleWrapper) CreateRole(ctx context.Context, roleName string,
 trustedUserArn string) (*types.Role, error) {
 var role *types.Role
 trustPolicy := PolicyDocument{
  Version: "2012-10-17",
  Statement: []PolicyStatement{{
   Effect:    "Allow",
   Principal: map[string]string{"AWS": trustedUserArn},
   Action:    []string{"sts:AssumeRole"},
  }},
 }
 policyBytes, err := json.Marshal(trustPolicy)
 if err != nil {
  log.Printf("Couldn't create trust policy for %v. Here's why: %v\n",
 trustedUserArn, err)
  return nil, err
 }
 result, err := wrapper.IamClient.CreateRole(ctx, &iam.CreateRoleInput{
  AssumeRolePolicyDocument: aws.String(string(policyBytes)),
  RoleName:                 aws.String(roleName),
 })
 if err != nil {
  log.Printf("Couldn't create role %v. Here's why: %v\n", roleName, err)
 } else {
  role = result.Role
 }
 return role, err
}
```

- Untuk detail API, lihat CreateRoledi Referensi AWS SDK untuk Go API.

Java

SDK untuk Java 2.x

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

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

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

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

                Where:
                    rolename - The name of the role to create.\s
                    fileLocation - The location of the JSON document that
 represents the trust policy.\s
                """;

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

        String rolename = args[0];
        String fileLocation = args[1];
        Region region = Region.AWS_GLOBAL;
```

```
        IamClient iam = IamClient.builder()
                .region(region)
                .build();

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

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

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

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

    public static Object readJsonSimpleDemo(String filename) throws Exception {
        FileReader reader = new FileReader(filename);
        JSONParser jsonParser = new JSONParser();
        return jsonParser.parse(reader);
    }
}
```

- Untuk detail API, lihat CreateRoledi Referensi AWS SDK for Java 2.x API.

JavaScript

SDK untuk JavaScript (v3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

Buat peran.

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

const client = new IAMClient({});

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

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

- Untuk detail API, lihat CreateRoledi Referensi AWS SDK untuk JavaScript API.

PHP

SDK untuk PHP

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

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

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

    /**
     * @param string $roleName
     * @param string $rolePolicyDocument
     * @return array
     * @throws AwsException
     */
    public function createRole(string $roleName, string $rolePolicyDocument)
    {
        $result = $this->customWaiter(function () use ($roleName,
 $rolePolicyDocument) {
            return $this->iamClient->createRole([
                'AssumeRolePolicyDocument' => $rolePolicyDocument,
                'RoleName' => $roleName,
            ]);
        });
        return $result['Role'];
    }
```

- Untuk detail API, lihat CreateRoledi Referensi AWS SDK untuk PHP API.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Contoh ini membuat peran baru bernama **MyNewRole** dan melampirkan padanya kebijakan yang ditemukan dalam file**NewRoleTrustPolicy.json**. Perhatikan bahwa Anda harus menggunakan parameter **-Raw** switch untuk berhasil memproses file kebijakan JSON. Dokumen kebijakan yang ditampilkan dalam output adalah URL yang dikodekan. Ini diterjemahkan dalam contoh ini dengan **UrlDecode** metode.NET.

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

Output:

```
Arn                       : arn:aws:iam::123456789012:role/MyNewRole
AssumeRolePolicyDocument : %7B%0D%0A%20%20%22Version%22%3A%20%222012-10-17%22%2C
%0D%0A%20%20%22Statement%22
                           %3A%20%5B%0D%0A%20%20%20%20%7B%0D%0A
%20%20%20%20%20%20%22Sid%22%3A%20%22%22%2C
                           %0D%0A%20%20%20%20%20%20%22Effect%22%3A%20%22Allow
%22%2C%0D%0A%20%20%20%20%20%20
                           %22Principal%22%3A%20%7B%0D%0A
%20%20%20%20%20%20%20%20%22AWS%22%3A%20%22arn%3Aaws
                           %3Aiam%3A%3A123456789012%3ADavid%22%0D%0A
%20%20%20%20%20%20%7D%2C%0D%0A%20%20%20
                           %20%20%20%22Action%22%3A%20%22sts%3AAssumeRole%22%0D
%0A%20%20%20%20%7D%0D%0A%20
                           %20%5D%0D%0A%7D
CreateDate                : 4/15/2015 11:04:23 AM
Path                      : /
RoleId                    : V5PAJI2KPN4EAEXAMPLE1
RoleName                  : MyNewRole

[System.Reflection.Assembly]::LoadWithPartialName("System.Web.HttpUtility")
```

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

- Untuk detail API, lihat CreateRoledi Referensi Alat AWS untuk PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Contoh ini membuat peran baru bernama **`MyNewRole`** dan melampirkan padanya kebijakan yang ditemukan dalam file**`NewRoleTrustPolicy.json`**. Perhatikan bahwa Anda harus menggunakan parameter **`-Raw`** switch untuk berhasil memproses file kebijakan JSON. Dokumen kebijakan yang ditampilkan dalam output adalah URL yang dikodekan. Ini diterjemahkan dalam contoh ini dengan **`UrlDecode`** metode.NET.

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

Output:

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

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

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

- Untuk detail API, lihat CreateRoledi Referensi Alat AWS untuk PowerShell Cmdlet (V5).

Python

SDK untuk Python (Boto3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

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

    :param role_name: The name of the role.
    :param allowed_services: The services that can assume the role.
```

```
    :return: The newly created role.
    """
    trust_policy = {
        "Version": "2012-10-17",
        "Statement": [
            {
                "Effect": "Allow",
                "Principal": {"Service": service},
                "Action": "sts:AssumeRole",
            }
            for service in allowed_services
        ],
    }

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

- Untuk detail API, lihat CreateRoledi AWS SDK for Python (Boto3) Referensi API.

Ruby

SDK untuk Ruby

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

```
# Creates a role and attaches policies to it.
#
```

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

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

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

- Untuk detail API, lihat CreateRoledi Referensi AWS SDK untuk Ruby API.

Rust

SDK untuk Rust

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

```
pub async fn create_role(
    client: &iamClient,
    role_name: &str,
```

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

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

- Untuk detail API, lihat CreateRolereferensi AWS SDK for Rust API.

Swift

SDK untuk Swift

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

```
import AWSIAM
import AWSS3


    public func createRole(name: String, policyDocument: String) async throws ->
 String {
        let input = CreateRoleInput(
            assumeRolePolicyDocument: policyDocument,
            roleName: name
        )
        do {
            let output = try await client.createRole(input: input)
```

```
            guard let role = output.role else {
                throw ServiceHandlerError.noSuchRole
            }
            guard let id = role.roleId else {
                throw ServiceHandlerError.noSuchRole
            }
            return id
        } catch {
            print("ERROR: createRole:", dump(error))
            throw error
        }
    }
```

- Untuk detail API, lihat referensi CreateRole AWSSDK untuk Swift API.

Dimulai AWS Config dengan perekam konfigurasi yang dikelola pelanggan menggunakan AWS CLI

Anda dapat memulai AWS Config dengan membuat perekam konfigurasi terkelola pelanggan. Untuk membuat perekam konfigurasi terkelola pelanggan dengan AWS CLI, gunakan perintah berikut: `put-configuration-recorder`, `put-delivery-channel`, dan `start-configuration-recorder`.

- `put-configuration-recorder`Perintah membuat perekam konfigurasi terkelola pelanggan.
- `put-delivery-channel`Perintah membuat saluran pengiriman tempat AWS Config mengirimkan informasi konfigurasi ke bucket S3 dan topik SNS.
- `start-configuration-recorder`Memulai perekam konfigurasi yang dikelola pelanggan. Perekam konfigurasi terkelola pelanggan akan mulai merekam perubahan konfigurasi untuk jenis sumber daya yang Anda tentukan.

Topik

- Pertimbangan
- Langkah 1: Jalankan put-configuration-recorder
- Langkah 2: Jalankan put-delivery-channel perintah
- Langkah 3: Jalankan start-configuration-recorder perintah

Pertimbangan

Bucket S3, topik SNS, dan peran IAM diperlukan

Untuk membuat perekam konfigurasi terkelola pelanggan, Anda perlu membuat bucket S3, topik SNS, dan peran IAM dengan kebijakan terlampir sebagai prasyarat. Untuk mengatur prasyarat Anda, lihat Prasyarat AWS Config.

Satu perekam konfigurasi terkelola pelanggan per akun per Wilayah

Anda hanya dapat memiliki satu perekam konfigurasi yang dikelola pelanggan Akun AWS untuk masing-masing perekam konfigurasi Wilayah AWS.

Satu saluran pengiriman per akun per Wilayah

Anda hanya dapat memiliki satu wilayah saluran pengiriman Akun AWS untuk masing-masing wilayah Wilayah AWS.

Kebijakan dan hasil kepatuhan

Kebijakan IAM dan kebijakan lain yang dikelola AWS Organizations dapat memengaruhi apakah AWS Config memiliki izin untuk merekam perubahan konfigurasi untuk sumber daya Anda. Selain itu, aturan secara langsung mengevaluasi konfigurasi sumber daya dan aturan tidak memperhitungkan kebijakan ini saat menjalankan evaluasi. Pastikan bahwa kebijakan yang berlaku selaras dengan cara Anda berniat untuk menggunakan AWS Config.

Langkah 1: Jalankan put-configuration-recorder

Gunakan `put-configuration-recorder`perintah untuk membuat perekam konfigurasi terkelola pelanggan:

Perintah ini menggunakan `--configuration-recorder` dan `---recording-group` bidang.

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

`configuration-recorder`Bidang

`configurationRecorder.json`File menentukan `name` dan `roleArn` serta frekuensi perekaman default untuk perekam konfigurasi (`recordingMode`). Anda juga dapat menggunakan bidang ini untuk mengganti frekuensi perekaman untuk jenis sumber daya tertentu.

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

`recording-group`Bidang

`recordingGroup.json`File menentukan jenis sumber daya yang direkam.

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

Untuk informasi selengkapnya tentang bidang ini, lihat `put-configuration-recorder`di Referensi AWS CLI Perintah.

Langkah 2: Jalankan put-delivery-channel perintah

Gunakan `put-delivery-channel`perintah untuk membuat saluran pengiriman:

Perintah ini menggunakan `--delivery-channel` bidang.

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

`delivery-channel`Bidang

`deliveryChannel.jsonFile` menentukan yang berikut:

- `name`Untuk saluran pengiriman.
- `s3BucketName`Tempat AWS Config mengirim snapshot konfigurasi.
- `snsTopicARN`Tempat AWS Config mengirim notifikasi
- `configSnapshotDeliveryProperties`Yang menetapkan seberapa sering AWS Config memberikan snapshot konfigurasi dan seberapa sering memanggil evaluasi untuk aturan periodik.

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

Untuk informasi selengkapnya tentang bidang ini, lihat `put-delivery-channel`di Referensi AWS CLI Perintah.

Langkah 3: Jalankan start-configuration-recorder perintah

Gunakan `start-configuration-recorder`perintah untuk memulai AWS Config:

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

Untuk informasi selengkapnya tentang bidang ini, lihat `start-configuration-recorder`di Referensi AWS CLI Perintah.

Memverifikasi bahwa Berhasil AWS Config Dimulai dengan AWS CLI

Setelah Anda mulai AWS Config, Anda dapat menggunakan AWS CLI perintah untuk memeriksa apakah AWS Config sedang berjalan dan yang AWS Config telah membuat perekam konfigurasi dan saluran pengiriman. Anda juga dapat mengonfirmasi bahwa AWS Config telah mulai merekam dan mengirimkan konfigurasi ke saluran pengiriman.

Topik

- Langkah 1: Periksa apakah saluran pengiriman dibuat
- Langkah 2: Periksa apakah perekam konfigurasi dibuat
- Langkah 3: Periksa apakah AWS Config sudah mulai merekam

Langkah 1: Periksa apakah saluran pengiriman dibuat

Gunakan `describe-delivery-channels`perintah untuk memeriksa apakah bucket Amazon S3 dan topik Amazon SNS Anda dikonfigurasi.

Anda dapat menggunakan `--delivery-channel-names` bidang untuk menentukan daftar saluran pengiriman. Jika saluran pengiriman tidak ditentukan, perintah ini mengembalikan rincian semua saluran pengiriman yang terkait dengan akun.

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

Langkah 2: Periksa apakah perekam konfigurasi dibuat

Gunakan `describe-configuration-recorders`perintah untuk memeriksa apakah perekam konfigurasi dibuat.

Anda dapat menggunakan `configuration-recorder-names` bidang `arn` dan untuk menentukan daftar perekam konfigurasi. Jika perekam konfigurasi tidak ditentukan, perintah ini mengembalikan detail semua perekam konfigurasi yang terkait dengan akun.

```
$ aws configservice describe-configuration-recorders
{
    "ConfigurationRecorders": [
        {
```

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

Langkah 3: Periksa apakah AWS Config sudah mulai merekam

Gunakan `describe-configuration-recorder-status`perintah untuk memeriksa apakah perekam konfigurasi berhasil merekam jenis sumber daya dalam ruang lingkup.

Anda dapat menggunakan `configuration-recorder-names` bidang `arn` dan untuk menentukan daftar perekam konfigurasi. Jika perekam konfigurasi tidak ditentukan, perintah ini mengembalikan detail semua perekam konfigurasi yang terkait dengan akun.

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

`true`Nilai di `recording` bidang menegaskan bahwa perekam konfigurasi telah mulai merekam konfigurasi. AWS Config mencatat waktu di UTC. Output ditampilkan sebagai stempel waktu Unix.

Menggunakan AWS Config dengan AWS SDK

AWS kit pengembangan perangkat lunak (SDKs) tersedia untuk banyak bahasa pemrograman populer. Setiap SDK menyediakan API, contoh kode, dan dokumentasi yang memudahkan developer untuk membangun aplikasi dalam bahasa pilihan mereka.

Dokumentasi SDK	Contoh kode
AWS SDK untuk C++	AWS SDK untuk C++ contoh kode
AWS CLI	AWS CLI contoh kode
AWS SDK untuk Go	AWS SDK untuk Go contoh kode
AWS SDK untuk Java	AWS SDK untuk Java contoh kode
AWS SDK untuk JavaScript	AWS SDK untuk JavaScript contoh kode
AWS SDK untuk Kotlin	AWS SDK untuk Kotlin contoh kode
AWS SDK untuk .NET	AWS SDK untuk .NET contoh kode
AWS SDK untuk PHP	AWS SDK untuk PHP contoh kode
Alat AWS untuk PowerShell	Alat AWS untuk PowerShell contoh kode
AWS SDK untuk Python (Boto3)	AWS SDK untuk Python (Boto3) contoh kode
AWS SDK untuk Ruby	AWS SDK untuk Ruby contoh kode
AWS SDK for Rust	AWS SDK for Rust contoh kode
AWS SDK untuk SAP ABAP	AWS SDK untuk SAP ABAP contoh kode
AWS SDK for Swift	AWS SDK for Swift contoh kode

Ketersediaan contoh

Tidak dapat menemukan apa yang Anda butuhkan? Minta contoh kode menggunakan tautan Berikan umpan balik di bagian bawah halaman ini.

Bekerja dengan perekam konfigurasi

Perekam konfigurasi menyimpan perubahan konfigurasi pada jenis sumber daya dalam lingkup sebagai item konfigurasi (CIs).

Ada dua jenis perekam konfigurasi.

Jenis	Deskripsi
Perekam konfigurasi terkelola pelanggan	Perekam konfigurasi yang Anda kelola. Jenis sumber daya dalam lingkup ditetapkan oleh Anda. Secara default, perekam konfigurasi terkelola pelanggan merekam semua sumber daya yang AWS Config didukung Wilayah AWS di tempat berjalan.
Perekam konfigurasi terkait layanan	Perekam konfigurasi yang ditautkan ke yang spesifik Layanan AWS. Jenis sumber daya dalam lingkup ditetapkan oleh layanan tertaut.

Topik

- Pertimbangan untuk perekam konfigurasi terkelola pelanggan
- Pertimbangan untuk perekam konfigurasi terkait layanan
- Deteksi drift untuk perekam konfigurasi
- Memulai perekam konfigurasi terkelola pelanggan
- Menghentikan perekam konfigurasi terkelola pelanggan
- Mengubah frekuensi perekaman untuk perekam konfigurasi terkelola pelanggan
- Mengganti nama perekam konfigurasi terkelola pelanggan
- Melihat perekam konfigurasi Anda
- Menghapus perekam konfigurasi Anda

Pertimbangan untuk perekam konfigurasi terkelola pelanggan

Satu perekam konfigurasi terkelola pelanggan per akun per Wilayah

Anda hanya dapat memiliki satu perekam konfigurasi yang dikelola pelanggan Akun AWS untuk masing-masing perekam konfigurasi Wilayah AWS.

Defaultnya adalah merekam semua jenis sumber daya yang didukung, tidak termasuk tipe sumber daya IAM global

Default untuk perekam konfigurasi terkelola pelanggan adalah merekam semua jenis sumber daya yang didukung, tidak termasuk jenis sumber daya IAM global berikut:`AWS::IAM::Group`,, `AWS::IAM::PolicyAWS::IAM::Role`, dan `AWS::IAM::User` Anda dapat menentukan jenis sumber daya yang ingin Anda sertakan atau kecualikan dari rekaman.

Untuk informasi selengkapnya, lihat Merekam AWS Sumber Daya dengan AWS Config.

Anda dikenakan biaya penggunaan layanan untuk menggunakan perekam konfigurasi terkelola pelanggan

Anda dikenakan biaya penggunaan layanan saat AWS Config mulai merekam konfigurasi dengan perekam konfigurasi terkelola pelanggan.

Untuk informasi harga, lihat Harga AWS Config.

Gunakan AWS Systems Manager untuk membuat perekam konfigurasi terkelola pelanggan di seluruh organisasi

Anda dapat menggunakan Pengaturan AWS Systems Manager Cepat untuk membuat perekam konfigurasi terkelola pelanggan di beberapa unit organisasi (OUs) dan Wilayah AWS menggunakan praktik AWS terbaik.

Untuk informasi selengkapnya, lihat Membuat perekam AWS Config konfigurasi menggunakan Pengaturan Cepat di Panduan Pengguna Systems Manager.

> **Important**
>
> Kebijakan dan hasil kepatuhan
> Kebijakan IAM dan kebijakan lain yang dikelola AWS Organizations dapat memengaruhi apakah AWS Config memiliki izin untuk merekam perubahan konfigurasi untuk sumber daya Anda. Selain itu, aturan secara langsung mengevaluasi konfigurasi sumber daya dan aturan tidak memperhitungkan kebijakan ini saat menjalankan evaluasi. Pastikan bahwa kebijakan yang berlaku selaras dengan cara Anda ingin menggunakan AWS Config.

Hasil evaluasi basi untuk sumber daya yang dihapus dapat bertahan jika perekam konfigurasi dimatikan
Jika perekam konfigurasi terkelola pelanggan dimatikan, itu menonaktifkan kemampuan AWS Config Config untuk melacak perubahan pada konfigurasi sumber daya yang Anda tentukan, termasuk penghapusannya. Ini berarti Anda mungkin melihat hasil evaluasi basi untuk sumber daya yang dihapus saat perekam konfigurasi terkelola pelanggan dimatikan karena AWS Config tidak dapat menangkap peristiwa penghapusan jika perekaman tidak aktif.

Pertimbangan untuk perekam konfigurasi terkait layanan

AWS Config Peran terkait layanan harus digunakan

Peran AWS Config terkait layanan diperlukan untuk perekam konfigurasi terkait layanan.

Untuk informasi selengkapnya, lihat Menggunakan Peran Tertaut Layanan untuk. AWS Config

Perekam konfigurasi terkait layanan selalu merekam

Anda tidak dapat menghentikan atau mulai merekam untuk perekam konfigurasi terkait layanan. Untuk berhenti merekam, Anda harus menghapus perekam konfigurasi terkait layanan.

Untuk informasi selengkapnya, lihat Menghapus Perekam Konfigurasi.

Lingkup perekaman menentukan apakah Anda menerima item konfigurasi

Lingkup perekaman diatur oleh layanan yang ditautkan ke perekam konfigurasi dan menentukan apakah Anda menerima item konfigurasi (CIs) di saluran pengiriman. Jika ruang lingkup perekaman internal, Anda tidak akan menerima CIs di saluran pengiriman.

Lingkup perekaman menentukan apakah Anda dikenakan biaya layanan

Lingkup perekaman diatur oleh layanan yang ditautkan ke perekam konfigurasi dan menentukan apakah item konfigurasi (CIs) dalam ruang lingkup dicatat secara gratis (INTERNAL) atau jika berdampak pada biaya tagihan Anda (DIBAYAR).

Layanan yang didukung

Perekam konfigurasi terkait layanan didukung untuk layanan berikut:

AWS layanan	Prinsipal layanan	Manfaat menggunakan dengan AWS Config	Pelajari selengkapnya
Amazon CloudWatch	`observabilityadmin.amazonaws.com`	Anda dapat menggunakan Amazon CloudWatch Observability Admin untuk menemukan dan memahami status konfigurasi telemetri CloudWatch untuk AWS Organisasi atau akun Anda.	Untuk informasi selengkapnya, lihat Mengaudit konfigurasi CloudWatch telemetri di Panduan Pengguna. CloudWatch
AWS Security Hub	`securityhub.amazonaws.com`	Anda dapat menggunakannya AWS Security Hub untuk mengelola temuan keamanan secara terpusat dan melakukan penilaian keamanan di seluruh akun Anda AWS . Perekam terkait layanan memungkinkan pendekatan berbasis peristiwa untuk mendapatkan item konfigurasi sumber daya yang diperlukan untuk cakupan analisis eksposur.	Untuk informasi selengkapnya, lihat Mengaktifkan Security Hub di Panduan Pengguna Security Hub.

Deteksi drift untuk perekam konfigurasi

Jenis `AWS::Config::ConfigurationRecorder` sumber daya adalah item konfigurasi (CI) untuk perekam konfigurasi yang melacak semua perubahan pada status perekam konfigurasi. Anda dapat menggunakan CI ini untuk memeriksa apakah status perekam konfigurasi berbeda, atau telah melayang, dari keadaan sebelumnya.

Misalnya, CI ini melacak jika ada pembaruan untuk jenis sumber daya yang telah Anda aktifkan AWS Config untuk dilacak, jika Anda telah menghentikan atau memulai perekam konfigurasi, atau jika Anda telah menghapus atau menghapus pemasangan perekam konfigurasi. Perekam konfigurasi hanyut menunjukkan bahwa Anda tidak secara akurat mendeteksi perubahan pada jenis sumber daya yang Anda inginkan. Jika perekam konfigurasi Anda telah hanyut, ini dapat menghasilkan hasil kepatuhan negatif palsu atau positif palsu.

Jenis `AWS::Config::ConfigurationRecorder` sumber daya adalah jenis sumber daya sistem AWS Config dan perekaman jenis sumber daya ini diaktifkan secara default di semua Wilayah yang didukung. Rekaman untuk jenis `AWS::Config::ConfigurationRecorder` sumber daya dilengkapi tanpa biaya tambahan.

Memulai perekam konfigurasi terkelola pelanggan

Anda dapat menggunakan AWS Config konsol atau AWS CLI memulai perekam konfigurasi yang dikelola pelanggan.

To start the customer managed configuration recorder (Console)

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Pilih Pengaturan di panel navigasi.
3. Pada tab Perekam terkelola pelanggan, pilih Mulai merekam. Saat diminta, pilih Konfirmasi.

To start the customer managed configuration recorder (CLI)

Gunakan `start-configuration-recorder`perintah:

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

Menghentikan perekam konfigurasi terkelola pelanggan

> **Note**
>
> Perekam konfigurasi terkait layanan selalu merekam
> Anda tidak dapat menghentikan perekam konfigurasi terkait layanan karena perekam konfigurasi terkait layanan selalu merekam. Untuk berhenti merekam, Anda harus menghapus perekam konfigurasi terkait layanan. Untuk informasi selengkapnya, lihat Menghapus Perekam Konfigurasi.

Anda dapat menggunakan AWS Config konsol atau AWS CLI menghentikan perekam konfigurasi yang dikelola pelanggan.

To stop the customer managed configuration recorder (Console)

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Pilih Pengaturan di panel navigasi.
3. Pada tab Perekam terkelola pelanggan, pilih Hentikan perekaman. Saat diminta, pilih Konfirmasi.

To stop the customer managed configuration recorder (CLI)

Gunakan `stop-configuration-recorder`perintah:

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

Mengubah frekuensi perekaman untuk perekam konfigurasi terkelola pelanggan

AWS Config mendukung perekaman terus menerus dan perekaman harian:

- Perekaman berkelanjutan memungkinkan Anda merekam perubahan konfigurasi secara terus menerus setiap kali terjadi perubahan.

- Rekaman harian memungkinkan Anda menerima item konfigurasi (CI) yang mewakili status terbaru sumber daya Anda selama periode 24 jam terakhir, hanya jika berbeda dari CI sebelumnya yang direkam. Untuk informasi lebih lanjut lihat, Frekuensi Perekaman.

Anda dapat menggunakan AWS Config konsol atau AWS CLI mengubah frekuensi perekaman.

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

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Pilih Pengaturan di panel navigasi.
3. Pada tab Perekam terkelola pelanggan, pilih Mulai merekam.
4. Untuk Perekam terkelola metode perekam, pilih Semua jenis sumber daya dengan penggantian yang dapat disesuaikan.
5. Untuk pengaturan Default, pilih frekuensi perekaman.
6. Pilih Simpan.

To change the recording frequency (CLI)

Gunakan `put-configuration-recorder`perintah untuk mengubah frekuensi perekaman untuk perekam konfigurasi:

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

`configurationRecorder.json`File menentukan `name` dan `roleArn` serta frekuensi perekaman default untuk perekam konfigurasi (`recordingMode`). Anda juga dapat menggunakan bidang ini untuk mengganti frekuensi perekaman untuk jenis sumber daya tertentu.

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
```

```
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include in
 the override ]
        }
    ]
  }
}
```

put-configuration-recordermenggunakan bidang berikut untuk `--configuration-recorder` parameter:

- `name`— Nama perekam konfigurasi. AWS Config secara otomatis menetapkan nama “default” saat membuat perekam konfigurasi.
- `roleARN`— Amazon Resource Name (ARN) dari peran IAM yang diasumsikan oleh AWS Config dan digunakan oleh perekam konfigurasi.
- `recordingMode`- Menentukan frekuensi perekaman default yang AWS Config digunakan untuk merekam perubahan konfigurasi. AWS Config mendukung perekaman berkelanjutan dan perekaman harian. Perekaman berkelanjutan memungkinkan Anda merekam perubahan konfigurasi secara terus menerus setiap kali terjadi perubahan. Rekaman harian memungkinkan Anda menerima item konfigurasi (CI) yang mewakili status terbaru sumber daya Anda selama periode 24 jam terakhir, hanya jika berbeda dari CI sebelumnya yang direkam.
  - `recordingFrequency`— Frekuensi perekaman default yang AWS Config digunakan untuk merekam perubahan konfigurasi.

    > **Note**
    >
    > AWS Firewall Manager tergantung pada perekaman berkelanjutan untuk memantau sumber daya Anda. Jika Anda menggunakan Firewall Manager, disarankan agar Anda mengatur frekuensi perekaman ke Continuous.

  - `recordingModeOverrides`— Bidang ini memungkinkan Anda untuk menentukan penggantian Anda untuk mode perekaman. Ini adalah array `recordingModeOverride` objek. Setiap `recordingModeOverride` objek dalam `recordingModeOverrides` array terdiri dari tiga bidang:
    - `description`— Deskripsi yang Anda berikan untuk penggantian.
    - `recordingFrequency`— Frekuensi perekaman yang akan diterapkan ke semua jenis sumber daya yang ditentukan dalam penggantian.

- `resourceTypes`— Daftar dipisahkan koma yang menentukan jenis sumber daya mana yang AWS Config termasuk dalam penggantian.

> **Note**
>
> Bidang wajib dan opsional
> `recordingMode`Bidang untuk `put-configuration-recorder`adalah opsional. Secara default, frekuensi perekaman untuk perekam konfigurasi diatur ke Perekaman berkelanjutan.

> **Note**
>
> Batas
> Rekaman harian tidak didukung untuk jenis sumber daya berikut:
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`
>
> Untuk strategi perekaman Record all current and future supported resource types (`ALL_SUPPORTED_RESOURCE_TYPES`), tipe resource ini akan diatur ke Continuous recording.

Mengganti nama perekam konfigurasi terkelola pelanggan

Anda harus menggunakan AWS CLI untuk mengganti nama perekam konfigurasi terkelola pelanggan. Untuk mengubah nama perekam konfigurasi terkelola pelanggan, Anda harus menghapusnya dan membuat perekam konfigurasi baru dengan nama yang Anda tentukan.

Mengganti nama perekam konfigurasi terkelola pelanggan menggunakan AWS CLI

1. Gunakan `describe-configuration-recorders`perintah untuk mencari nama perekam konfigurasi terkelola pelanggan Anda saat ini:

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

2. Gunakan `delete-configuration-recorder`perintah untuk menghapus perekam konfigurasi saat ini yang dikelola pelanggan Anda:

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

3. Gunakan `put-configuration-recorder`perintah untuk membuat perekam konfigurasi terkelola pelanggan dengan nama baru:

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

4. Gunakan `start-configuration-recorder`perintah untuk melanjutkan perekaman:

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

Melihat perekam konfigurasi Anda

Anda dapat menggunakan AWS Config konsol atau detail AWS CLI tampilan tentang perekam konfigurasi Anda.

To view your configuration recorders (Console)

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Pilih Pengaturan di panel navigasi.

3. Untuk perekam konfigurasi terkelola pelanggan, Anda dapat melihat detail di tab Perekam terkelola pelanggan.
4. Untuk perekam konfigurasi terkait layanan, pilih perekam konfigurasi terkait layanan pada tab Perekam terkait layanan, lalu pilih Lihat.

To view your configuration recorders (CLI)

Gunakan `describe-configuration-recorders`perintah untuk melihat detail tentang perekam konfigurasi Anda:

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

Gunakan `describe-configuration-recorder-status`perintah untuk melihat status perekam konfigurasi Anda saat ini:

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

Untuk kedua perintah ini, Anda dapat menggunakan `configuration-recorder-names` bidang `arn` dan untuk menentukan daftar perekam konfigurasi. Untuk perekam konfigurasi terkait

layanan, Anda dapat menggunakan `service-principal` bidang untuk menentukan perekam konfigurasi.

Jika perekam konfigurasi tidak ditentukan, perintah ini mengembalikan detail semua perekam konfigurasi yang terkait dengan akun.

Menghapus perekam konfigurasi Anda

Anda harus menggunakan AWS CLI untuk menghapus perekam konfigurasi terkelola pelanggan. Anda dapat menggunakan AWS Config konsol atau AWS CLI untuk menghapus perekam konfigurasi terkait layanan.

To delete the customer managed configuration recorder (CLI)

Gunakan `delete-configuration-recorder`perintah:

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

To delete a service-linked configuration recorder (Console)

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Pilih Pengaturan di panel navigasi.
3. Pada tab Perekam terkait layanan, pilih perekam konfigurasi terkait layanan pada tab Perekam terkait layanan, lalu pilih Hapus. Saat diminta, pilih Hapus.

To delete a service-linked configuration recorder (CLI)

Gunakan `delete-service-linked-configuration-recorder`perintah:

Perintah ini menggunakan `--service-principal` bidang.

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

Bekerja dengan Delivery Channel

Karena AWS Config terus-menerus mencatat perubahan yang terjadi pada AWS sumber daya Anda, ia mengirimkan pemberitahuan dan status konfigurasi yang diperbarui melalui saluran pengiriman. Anda dapat mengelola saluran pengiriman untuk mengontrol tempat AWS Config mengirim pembaruan konfigurasi.

Topik

- Pertimbangan
- Terminologi
- Komponen Item Konfigurasi
- Melihat Saluran Pengiriman
- Memperbarui Saluran Pengiriman
- Mengganti nama Saluran Pengiriman
- Mengirimkan Snapshot Konfigurasi ke Bucket Amazon S3
- Memverifikasi Status Pengiriman
- Melihat Snapshot Konfigurasi di bucket Amazon S3
- Contoh Konfigurasi Snapshot dari AWS Config
- Pemberitahuan yang AWS Config Mengirim ke topik Amazon SNS

Pertimbangan

Satu saluran pengiriman per Wilayah per akun

Anda hanya dapat memiliki satu saluran pengiriman per AWS wilayah Wilayah per Akun AWS, dan saluran pengiriman harus digunakan AWS Config.

Pemberitahuan item konfigurasi yang terlalu besar mencakup ringkasan singkat

Saat AWS Config mendeteksi perubahan konfigurasi untuk sumber daya dan notifikasi melebihi ukuran maksimum yang diizinkan oleh Amazon SNS, pemberitahuan tersebut menyertakan ringkasan singkat item konfigurasi. Anda dapat melihat notifikasi lengkap di lokasi bucket Amazon S3 yang ditentukan di bidang. `s3BucketLocation` Untuk informasi selengkapnya, lihat Contoh Pemberitahuan Perubahan Item Konfigurasi Besar.

AWS Config mendukung AWS KMS enkripsi untuk bucket Amazon S3 yang digunakan oleh AWS Config

Anda dapat memberikan kunci AWS Key Management Service (AWS KMS) atau alias Nama Sumber Daya Amazon (ARN) untuk mengenkripsi data yang dikirimkan ke bucket Amazon Simple Storage Service (Amazon S3). Secara default, AWS Config mengirimkan riwayat konfigurasi dan file snapshot ke bucket Amazon S3 Anda dan mengenkripsi data saat istirahat menggunakan enkripsi sisi server S3 AES-256, SSE-S3. Namun, jika Anda menyediakan AWS Config kunci KMS atau alias ARN Anda, AWS Config gunakan kunci KMS itu alih-alih enkripsi AES-256.

AWS Config tidak mendukung saluran pengiriman ke bucket Amazon S3 di mana kunci objek diaktifkan dengan retensi default diaktifkan. Untuk informasi selengkapnya, lihat Cara kerja Kunci Objek S3.

Terminologi

Item konfigurasi mewakili point-in-time tampilan berbagai atribut AWS sumber daya yang didukung yang ada di akun Anda. Komponen item konfigurasi termasuk metadata, atribut, hubungan, konfigurasi saat ini, dan peristiwa terkait. AWS Config membuat item konfigurasi setiap kali mendeteksi perubahan pada jenis sumber daya yang direkam. Misalnya, jika AWS Config merekam bucket Amazon S3, AWS Config buat item konfigurasi setiap kali bucket dibuat, diperbarui, atau dihapus. Anda juga dapat memilih AWS Config untuk membuat item konfigurasi pada frekuensi perekaman yang Anda atur.

Riwayat konfigurasi adalah kumpulan item konfigurasi untuk sumber daya tertentu selama periode waktu apa pun. Riwayat konfigurasi dapat membantu Anda menjawab pertanyaan tentang, misalnya, kapan sumber daya pertama kali dibuat, bagaimana sumber daya telah dikonfigurasi selama sebulan terakhir, dan perubahan konfigurasi apa yang diperkenalkan kemarin pukul 9 pagi. Riwayat konfigurasi tersedia untuk Anda dalam berbagai format. AWS Config secara otomatis mengirimkan file riwayat konfigurasi untuk setiap jenis sumber daya yang direkam ke bucket Amazon S3 yang Anda tentukan. Anda dapat memilih sumber daya tertentu di AWS Config konsol dan menavigasi ke semua item konfigurasi sebelumnya untuk sumber daya tersebut menggunakan timeline. Selain itu, Anda dapat mengakses item konfigurasi historis untuk sumber daya dari API.

Snapshot konfigurasi adalah kumpulan item konfigurasi untuk sumber daya yang didukung yang ada di akun Anda. Snapshot konfigurasi ini adalah gambaran lengkap dari sumber daya yang sedang direkam dan konfigurasinya. Snapshot konfigurasi dapat menjadi alat yang berguna untuk memvalidasi konfigurasi Anda. Misalnya, Anda mungkin ingin memeriksa snapshot konfigurasi secara teratur untuk sumber daya yang dikonfigurasi secara tidak benar atau yang berpotensi tidak

ada. Snapshot konfigurasi tersedia dalam berbagai format. Snapshot konfigurasi dapat dikirimkan ke bucket Amazon Simple Storage Service (Amazon S3) yang ditentukan. Selain itu, Anda dapat memilih titik waktu di AWS Config konsol dan menavigasi snapshot item konfigurasi menggunakan hubungan antar sumber daya.

Aliran konfigurasi adalah daftar yang diperbarui secara otomatis dari semua item konfigurasi untuk sumber daya AWS Config yang direkam. Setiap kali sumber daya dibuat, dimodifikasi, atau dihapus, AWS Config buat item konfigurasi dan tambahkan ke aliran konfigurasi. Aliran konfigurasi berfungsi dengan menggunakan topik Amazon Simple Notification Service (Amazon SNS) pilihan Anda. Aliran konfigurasi sangat membantu untuk mengamati perubahan konfigurasi saat terjadi sehingga Anda dapat menemukan potensi masalah, menghasilkan pemberitahuan jika sumber daya tertentu diubah, atau memperbarui sistem eksternal yang perlu mencerminkan konfigurasi sumber AWS daya Anda.

Komponen Item Konfigurasi

Item konfigurasi mewakili point-in-time tampilan berbagai atribut AWS sumber daya yang didukung yang ada di akun Anda. Komponen item konfigurasi termasuk metadata, atribut, hubungan, konfigurasi saat ini, dan peristiwa terkait. AWS Config membuat item konfigurasi setiap kali mendeteksi perubahan pada jenis sumber daya yang direkam. Misalnya, jika AWS Config merekam bucket Amazon S3, AWS Config buat item konfigurasi setiap kali bucket dibuat, diperbarui, atau dihapus. Anda juga dapat memilih AWS Config untuk membuat item konfigurasi pada frekuensi perekaman yang Anda atur.

Item konfigurasi terdiri dari komponen-komponen berikut.

Komponen	Deskripsi	Contains
Metadata	Informasi tentang item konfigurasi ini	• ID Versi • Waktu ketika item konfigurasi ditangkap • Status item konfigurasi yang menunjukkan apakah item berhasil ditangkap • ID negara yang menunjukkan urutan item konfigurasi sumber daya
Atribut	Atribut sumber daya	• ID Sumber Daya • Daftar tag kunci-nilai untuk sumber daya ini

Komponen	Deskripsi	Contains
		• Jenis sumber daya (lihatJenis Sumber Daya yang Didukung untuk AWS Config) • Amazon Resource Name (ARN) • Availability Zone yang berisi sumber daya ini, jika berlaku • Waktu sumber daya dibuat
Hubungan	Bagaimana sumber daya terkait dengan sumber daya lain yang terkait dengan akun	Deskripsi hubungan, seperti volume Amazon EBS `vol-1234567` dilampirkan ke instans Amazon EC2 `i-a1b2c3d4`
Konfigurasi saat ini	Informasi yang dikembali kan melalui panggilan ke API Deskripsikan atau Daftar sumber daya	Misalnya, `DescribeVolumes` API mengembalikan informasi berikut tentang volume: • Availability Zone volume berada • Waktu volume terpasang • ID dari EC2 instance yang dilampirkan • Status volume saat ini • Keadaan DeleteOnTermination bendera • Perangkat volume terpasang • Jenis volume, seperti `gp2, io1,` atau `standard`

Catatan

1. Hubungan item konfigurasi tidak termasuk aliran jaringan atau dependensi aliran data. Item konfigurasi tidak dapat disesuaikan untuk mewakili arsitektur aplikasi Anda.
2. Pada Versi 1.3, bidang relateDevents kosong. Anda dapat mengakses LookupEvents API di Referensi AWS CloudTrail API untuk mengambil peristiwa untuk sumber daya.
3. Pada Versi 1.3, bidang ConfigurationItem MD5 Hash kosong. Anda dapat menggunakan configurationStateId bidang untuk memastikan Anda memiliki item konfigurasi terbaru.

4. Jika tipe sumber daya tidak mendukung penandaan atau tidak menyertakan informasi tag dalam respons API deskripsinya, tidak AWS Config akan menangkap data tag dalam item konfigurasi (CIs) untuk jenis sumber daya tersebut. AWS Config masih akan mencatat sumber daya ini. Namun, fungsionalitas apa pun yang bergantung pada data tag tidak akan berfungsi. Ini memengaruhi pemfilteran, pengelompokan, atau evaluasi kepatuhan berbasis tag yang bergantung pada data tag.

Melihat Saluran Pengiriman

Anda harus menggunakan AWS CLI untuk melihat detail tentang saluran pengiriman.

Contoh kode berikut menunjukkan cara menggunakan`DescribeDeliveryChannels`.

CLI

AWS CLI

Untuk mendapatkan detail tentang saluran pengiriman

Perintah berikut mengembalikan rincian tentang saluran pengiriman:

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

Output:

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

- Untuk detail API, lihat DescribeDeliveryChannelsdi Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Contoh ini mengambil saluran pengiriman untuk wilayah tersebut dan menampilkan detailnya.

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

Output:

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

- Untuk detail API, lihat DescribeDeliveryChannelsdi Referensi Alat AWS untuk PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Contoh ini mengambil saluran pengiriman untuk wilayah tersebut dan menampilkan detailnya.

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

Output:

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

- Untuk detail API, lihat DescribeDeliveryChannelsdi Referensi Alat AWS untuk PowerShell Cmdlet (V5).

Memperbarui Saluran Pengiriman

Saat memperbarui saluran pengiriman, Anda dapat mengatur opsi berikut:

- Bucket Amazon S3 tempat AWS Config mengirimkan snapshot konfigurasi dan file riwayat konfigurasi.
- Seberapa sering AWS Config mengirimkan snapshot konfigurasi ke bucket Amazon S3 Anda.
- Topik Amazon SNS yang AWS Config mengirimkan pemberitahuan tentang perubahan konfigurasi.

Untuk memperbarui saluran pengiriman (Konsol)

Anda dapat menggunakan AWS Config konsol untuk mengatur bucket Amazon S3 dan topik Amazon SNS untuk saluran pengiriman Anda. Untuk langkah-langkah mengelola pengaturan ini, lihatMenyiapkan AWS Config dengan Konsol.

Konsol tidak menyediakan opsi untuk mengganti nama saluran pengiriman, mengatur frekuensi untuk snapshot konfigurasi, atau menghapus saluran pengiriman. Untuk melakukan tugas-tugas ini, Anda harus menggunakan, AWS Config API, atau salah satu AWS SDKs. AWS CLI

Untuk memperbarui saluran pengiriman (AWS SDKs)

Contoh kode berikut menunjukkan cara menggunakan`PutDeliveryChannel`.

CLI

AWS CLI

Untuk membuat saluran pengiriman

Perintah berikut menyediakan pengaturan untuk saluran pengiriman sebagai kode JSON:

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

`deliveryChannel.json`File menentukan atribut saluran pengiriman:

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

Contoh ini menetapkan atribut berikut:

`name`- Nama saluran pengiriman. Secara default, AWS Config menetapkan nama `default` ke saluran pengiriman baru. Anda tidak dapat memperbarui nama saluran pengiriman dengan perintah. `put-delivery-channel` Untuk langkah-langkah mengubah nama, lihat Mengganti nama Saluran Pengiriman. `s3BucketName` - Nama bucket Amazon S3 tempat AWS Config memberikan snapshot konfigurasi dan file riwayat konfigurasi. Jika Anda menentukan bucket milik AWS akun lain, bucket tersebut harus memiliki kebijakan yang memberikan izin akses ke Config. AWS Untuk informasi selengkapnya, lihat Izin untuk Bucket Amazon S3.

`snsTopicARN`- Nama Sumber Daya Amazon (ARN) dari topik Amazon SNS tempat AWS Config mengirimkan pemberitahuan tentang perubahan konfigurasi. Jika Anda memilih topik dari akun lain, topik tersebut harus memiliki kebijakan yang memberikan izin akses ke Config. AWS Untuk informasi selengkapnya, lihat Izin untuk Topik Amazon SNS.

`configSnapshotDeliveryProperties`- Berisi `deliveryFrequency` atribut, yang menetapkan seberapa sering AWS Config memberikan snapshot konfigurasi dan seberapa sering ia memanggil evaluasi untuk aturan Config periodik.

Jika perintah berhasil, AWS Config tidak mengembalikan output. Untuk memverifikasi pengaturan saluran pengiriman Anda, jalankan describe-delivery-channels perintah.

- Untuk detail API, lihat PutDeliveryChannel di Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Contoh ini mengubah properti DeliveryFrequency dari saluran pengiriman yang ada.

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

- Untuk detail API, lihat PutDeliveryChannel di Referensi Alat AWS untuk PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Contoh ini mengubah properti DeliveryFrequency dari saluran pengiriman yang ada.

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

- Untuk detail API, lihat PutDeliveryChannelDi Referensi Alat AWS untuk PowerShell Cmdlet (V5).

(Opsional) Anda dapat menggunakan `describe-delivery-channels`perintah untuk memverifikasi bahwa pengaturan saluran pengiriman diperbarui:

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

Contoh kode berikut menunjukkan cara menggunakan`DescribeDeliveryChannels`.

CLI

AWS CLI

Untuk mendapatkan detail tentang saluran pengiriman

Perintah berikut mengembalikan rincian tentang saluran pengiriman:

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

Output:

```
{
    "DeliveryChannels": [
        {
```

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

- Untuk detail API, lihat DescribeDeliveryChannelsdi Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Contoh ini mengambil saluran pengiriman untuk wilayah tersebut dan menampilkan detailnya.

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

Output:

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

- Untuk detail API, lihat DescribeDeliveryChannelsdi Referensi Alat AWS untuk PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Contoh ini mengambil saluran pengiriman untuk wilayah tersebut dan menampilkan detailnya.

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

Output:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
```

```
----    ------------                ----------- -----------------
default config-bucket-NA my           TwentyFour_Hours
```

- Untuk detail API, lihat DescribeDeliveryChannelsdi Referensi Alat AWS untuk PowerShell Cmdlet (V5).

Mengganti nama Saluran Pengiriman

Untuk mengubah nama saluran pengiriman, Anda harus menghapusnya dan membuat saluran pengiriman baru dengan nama yang Anda tentukan. Sebelum Anda dapat menghapus saluran pengiriman, Anda harus menghentikan sementara perekam konfigurasi. AWS Config Konsol tidak menyediakan opsi untuk menghapus saluran pengiriman. Anda harus menggunakan AWS CLI, AWS Config API, atau salah satu. AWS SDKs

Mengganti nama saluran pengiriman menggunakan AWS CLI

1. Gunakan `stop-configuration-recorder`perintah untuk menghentikan perekam konfigurasi:

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

2. Gunakan `describe-delivery-channels`perintah, dan catat atribut saluran pengiriman Anda:

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

3. Gunakan `delete-delivery-channel`perintah untuk menghapus saluran pengiriman:

```
$ aws configservice delete-delivery-channel --delivery-channel-name default
```

4. Gunakan `put-delivery-channel`perintah untuk membuat saluran pengiriman dengan nama yang diinginkan:

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

File DeliveryChannel.json menentukan atribut saluran pengiriman:

```
{
    "name": "myCustomDeliveryChannelName",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

5. Gunakan `start-configuration-recorder` perintah untuk melanjutkan perekaman:

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

Mengirimkan Snapshot Konfigurasi ke Bucket Amazon S3

Snapshot konfigurasi adalah kumpulan item konfigurasi untuk sumber daya yang didukung yang ada di akun Anda. Snapshot konfigurasi ini adalah gambaran lengkap dari sumber daya yang sedang direkam dan konfigurasinya. Snapshot konfigurasi dapat menjadi alat yang berguna untuk memvalidasi konfigurasi Anda. Misalnya, Anda mungkin ingin memeriksa snapshot konfigurasi secara teratur untuk sumber daya yang dikonfigurasi secara tidak benar atau yang berpotensi tidak ada. Snapshot konfigurasi tersedia dalam berbagai format. Snapshot konfigurasi dapat dikirimkan ke bucket Amazon Simple Storage Service (Amazon S3) yang ditentukan. Selain itu, Anda dapat memilih titik waktu di AWS Config konsol dan menavigasi snapshot item konfigurasi menggunakan hubungan antar sumber daya.

Mengirimkan Snapshot Konfigurasi

AWS Config menghasilkan snapshot konfigurasi saat Anda menjalankan DeliverConfigSnapshottindakan atau Anda menjalankan perintah. AWS CLI `deliver-config-`

`snapshot` AWS Config menyimpan snapshot konfigurasi di bucket Amazon S3 yang Anda tentukan saat Anda mengaktifkan. AWS Config

Masukkan `deliver-config-snapshot`perintah dengan menentukan nama yang ditetapkan AWS Config saat Anda mengonfigurasi saluran pengiriman, misalnya:

```
$ aws configservice deliver-config-snapshot --delivery-channel-name default
{
    "configSnapshotId": "94ccff53-83be-42d9-996f-b4624b3c1a55"
}
```

Memverifikasi Status Pengiriman

Masukkan `describe-delivery-channel-status`perintah untuk memverifikasi bahwa AWS Config telah mulai mengirimkan konfigurasi ke saluran pengiriman yang ditentukan:

```
aws configservice describe-delivery-channel-status
```

Respons mencantumkan status ketiga format pengiriman yang AWS Config digunakan untuk mengirimkan konfigurasi ke bucket dan topik Anda.

```
{
    "DeliveryChannelsStatus": [
        {
            "configStreamDeliveryInfo": {
                "lastStatusChangeTime": 1415138614.125,
                "lastStatus": "SUCCESS"
            },
            "configHistoryDeliveryInfo": {
                "lastSuccessfulTime": 1415148744.267,
                "lastStatus": "SUCCESS",
                "lastAttemptTime": 1415148744.267
            },
            "configSnapshotDeliveryInfo": {
                "lastSuccessfulTime": 1415333113.4159999,
                "lastStatus": "SUCCESS",
                "lastAttemptTime": 1415333113.4159999
            },
            "name": "default"
        }
```

```
    ]
}
```

Lihat `lastSuccessfulTime` bidang di`configSnapshotDeliveryInfo`. Waktu harus sesuai dengan waktu terakhir Anda meminta pengiriman snapshot konfigurasi.

> **Note**
>
> AWS Config menggunakan format UTC (Coordinated Universal Time) untuk merekam waktu.

Melihat Snapshot Konfigurasi di bucket Amazon S3

Snapshot konfigurasi adalah kumpulan item konfigurasi untuk sumber daya yang didukung yang ada di akun Anda. Snapshot konfigurasi ini adalah gambaran lengkap dari sumber daya yang sedang direkam dan konfigurasinya. Snapshot konfigurasi dapat menjadi alat yang berguna untuk memvalidasi konfigurasi Anda. Misalnya, Anda mungkin ingin memeriksa snapshot konfigurasi secara teratur untuk sumber daya yang dikonfigurasi secara tidak benar atau yang berpotensi tidak ada. Snapshot konfigurasi tersedia dalam berbagai format. Snapshot konfigurasi dapat dikirimkan ke bucket Amazon Simple Storage Service (Amazon S3) yang ditentukan. Selain itu, Anda dapat memilih titik waktu di AWS Config konsol dan menavigasi snapshot item konfigurasi menggunakan hubungan antar sumber daya.

Melihat Snapshot Konfigurasi

1. Masuk ke AWS Management Console dan buka konsol Amazon S3 di. https://console.aws.amazon.com/s3/
2. Di daftar All Bucket konsol Amazon S3, pilih nama bucket Amazon S3 Anda.
3. Buka folder bersarang di bucket hingga Anda melihat `ConfigSnapshot` objek dengan ID snapshot yang cocok dengan ID yang dikembalikan oleh perintah. Unduh dan buka objek untuk melihat snapshot konfigurasi.. Bucket S3 juga berisi file kosong bernama`ConfigWritabilityCheckFile`. AWS Config membuat file ini untuk memverifikasi bahwa layanan dapat berhasil menulis ke bucket S3.

Contoh Konfigurasi Snapshot dari AWS Config

Berikut ini adalah contoh informasi yang AWS Config disertakan dalam snapshot konfigurasi. Snapshot menjelaskan konfigurasi untuk sumber daya yang AWS Config merekam di wilayah saat ini untuk Anda Akun AWS, dan menjelaskan hubungan antara sumber daya ini.

> **Note**
>
> Snapshot konfigurasi dapat menyertakan referensi ke jenis sumber daya dan sumber daya IDs yang tidak didukung.


```
{
    "fileVersion": "1.0",
    "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
    "configurationItems": [
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
            "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
```

```
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume1"
                    }
                ],
                "volumeType": "standard"
            }
        },
        {
            "configurationItemVersion": "1.0",
            "resourceId": "i-344c463d",
            "accountId": "12345678910",
            "arn": "arn:aws:ec2:us-west-2b:123456789012:instance/i-344c463d",
            "configurationItemCaptureTime": "2014-03-07T23:47:09.523Z",
            "configurationStateID": "cdb571fa-ce7a-4ec5-8914-0320466a355e",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Instance",
            "resourceCreationTime": "2014-02-26T22:56:35.000Z",
            "tags": {
                "Name": "integ-test-1",
```

```
                "examplename": "examplevalue"
            },
            "relationships": [
                {
                    "resourceId": "vol-ce676ccc",
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Attached Volume"
                },
                {
                    "resourceId": "vol-ef0e06ed",
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Attached Volume",
                    "direction": "OUT"
                },
                {
                    "resourceId": "subnet-47b4cf2c",
                    "resourceType": "AWS::EC2::SUBNET",
                    "name": "Is contained in Subnet",
                    "direction": "IN"
                }
            ],
            "configuration": {
                "instanceId": "i-344c463d",
                "imageId": "ami-ccf297fc",
                "state": {
                    "code": 16,
                    "name": "running"
                },
                "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
                "publicDnsName": "ec2-54-218-4-189.us-west-2.compute.amazonaws.com",
                "stateTransitionReason": "",
                "keyName": "configDemo",
                "amiLaunchIndex": 0,
                "productCodes": [],
                "instanceType": "t1.micro",
                "launchTime": "2014-02-26T22:56:35.0000+0000",
                "placement": {
                    "availabilityZone": "us-west-2b",
                    "groupName": "",
                    "tenancy": "default"
                },
                "kernelId": "aki-fc8f11cc",
                "monitoring": {
                    "state": "disabled"
```

```
                },
                "subnetId": "subnet-47b4cf2c",
                "vpcId": "vpc-41b4cf2a",
                "privateIpAddress": "172.31.21.63",
                "publicIpAddress": "54.218.4.189",
                "architecture": "x86_64",
                "rootDeviceType": "ebs",
                "rootDeviceName": "/dev/sda1",
                "blockDeviceMappings": [
                    {
                        "deviceName": "/dev/sda1",
                        "ebs": {
                            "volumeId": "vol-ef0e06ed",
                            "status": "attached",
                            "attachTime": "2014-02-26T22:56:38.0000+0000",
                            "deleteOnTermination": true
                        }
                    },
                    {
                        "deviceName": "/dev/sdf",
                        "ebs": {
                            "volumeId": "vol-ce676ccc",
                            "status": "attached",
                            "attachTime": "2014-03-07T23:46:28.0000+0000",
                            "deleteOnTermination": false
                        }
                    }
                ],
                "virtualizationType": "paravirtual",
                "clientToken": "aBCDe123456",
                "tags": [
                    {
                        "key": "Name",
                        "value": "integ-test-1"
                    },
                    {
                        "key": "examplekey",
                        "value": "examplevalue"
                    }
                ],
                "securityGroups": [
                    {
                        "groupName": "launch-wizard-2",
                        "groupId": "sg-892adfec"
```

```
                    }
                ],
                "sourceDestCheck": true,
                "hypervisor": "xen",
                "networkInterfaces": [
                    {
                        "networkInterfaceId": "eni-55c03d22",
                        "subnetId": "subnet-47b4cf2c",
                        "vpcId": "vpc-41b4cf2a",
                        "description": "",
                        "ownerId": "12345678910",
                        "status": "in-use",
                        "privateIpAddress": "172.31.21.63",
                        "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
                        "sourceDestCheck": true,
                        "groups": [
                            {
                                "groupName": "launch-wizard-2",
                                "groupId": "sg-892adfec"
                            }
                        ],
                        "attachment": {
                            "attachmentId": "eni-attach-bf90c489",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2014-02-26T22:56:35.0000+0000",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.218.4.189",
                            "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [
                            {
                                "privateIpAddress": "172.31.21.63",
                                "privateDnsName": "ip-172-31-21-63.us-
west-2.compute.internal",
                                "primary": true,
                                "association": {
                                    "publicIp": "54.218.4.189",
                                    "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
```

```
                                    "ipOwnerId": "amazon"
                                }
                            }
                        ]
                    }
                ],
                "ebsOptimized": false
            }
        }
    ]
}
```

Langkah selanjutnya adalah memverifikasi bahwa snapshot konfigurasi berhasil dikirim ke saluran pengiriman.

Pemberitahuan yang AWS Config Mengirim ke topik Amazon SNS

> **Note**
>
> Sebelum AWS Config dapat mengirim pemberitahuan ke topik Amazon SNS, Anda harus terlebih dahulu mengatur perekam konfigurasi dan saluran pengiriman. Untuk informasi selengkapnya, lihat Mengelola Perekam Konfigurasi dan Mengelola Saluran Pengiriman.

Anda dapat mengonfigurasi AWS Config untuk mengalirkan perubahan konfigurasi dan pemberitahuan ke topik Amazon SNS. Misalnya, ketika sumber daya diperbarui, Anda bisa mendapatkan pemberitahuan yang dikirim ke email Anda, sehingga Anda dapat melihat perubahan tersebut. Anda juga dapat diberi tahu saat AWS Config mengevaluasi aturan kustom atau terkelola terhadap sumber daya Anda. Untuk informasi selengkapnya, lihat Logging and Monitoring in AWS Config.

AWS Config mengirimkan pemberitahuan untuk acara berikut:

- Perubahan item konfigurasi untuk sumber daya.
- Riwayat konfigurasi untuk sumber daya dikirimkan ke akun Anda.
- Snapshot konfigurasi untuk sumber daya yang direkam dimulai dan dikirimkan untuk akun Anda.
- Status kepatuhan sumber daya Anda dan apakah mereka sesuai dengan aturan Anda.
- Evaluasi dimulai untuk aturan terhadap sumber daya Anda.

- AWS Config gagal mengirimkan notifikasi ke akun Anda.

Topik

- Contoh Pemberitahuan Perubahan Item Konfigurasi
- Contoh Pemberitahuan Pengiriman Riwayat Konfigurasi
- Contoh Konfigurasi Pengiriman Snapshot Mulai Pemberitahuan
- Contoh Konfigurasi Pemberitahuan Pengiriman Snapshot
- Contoh Pemberitahuan Perubahan Kepatuhan
- Contoh Aturan Evaluasi Mulai Pemberitahuan
- Contoh Pemberitahuan Perubahan Item Konfigurasi Besar
- Contoh Pemberitahuan Gagal Pengiriman

Contoh Pemberitahuan Perubahan Item Konfigurasi

AWS Config menggunakan Amazon SNS untuk mengirimkan pemberitahuan ke titik akhir berlangganan. Pemberitahuan ini memberikan status pengiriman untuk snapshot konfigurasi dan riwayat konfigurasi, dan pemberitahuan tersebut menyediakan setiap item konfigurasi yang AWS Config dibuat saat konfigurasi sumber daya yang direkam AWS berubah. AWS Config juga mengirimkan pemberitahuan yang menunjukkan apakah sumber daya Anda sesuai dengan aturan Anda. Jika Anda memilih untuk memiliki pemberitahuan yang dikirim melalui email, Anda dapat menggunakan filter dalam aplikasi klien email Anda berdasarkan baris subjek dan badan pesan email.

Berikut ini adalah contoh payload notifikasi Amazon SNS yang dihasilkan AWS Config saat mendeteksi bahwa `vol-ce676ccc` volume Amazon Elastic Block Store dilampirkan ke instance dengan ID sebesar. `i-344c463d` Pemberitahuan berisi perubahan item konfigurasi untuk sumber daya.

```
{
    "Type": "Notification",
    "MessageId": "8b945cb0-db34-5b72-b032-1724878af488",
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:example",
    "Message": {
        "MessageVersion": "1.0",
        "NotificationCreateTime": "2014-03-18T10:11:00Z",
        "messageType": "ConfigurationItemChangeNotification",
```

```
        "configurationItem": [
            {
                "configurationItemVersion": "1.0",
                "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
                "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
                "resourceId": "vol-ce676ccc",
                "awsAccountId": "123456789012",
                "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
                "configurationItemStatus": "OK",
                "relatedEvents": [],
                "availabilityZone": "us-west-2b",
                "resourceType": "AWS::EC2::VOLUME",
                "resourceCreationTime": "2014-02-27T21:43:53.885Z",
                "tags": {},
                "relationships": [
                    {
                        "resourceId": "i-344c463d",
                        "resourceType": "AWS::EC2::INSTANCE",
                        "name": "Attached to Instance"
                    }
                ],
                "configuration": {
                    "volumeId": "vol-ce676ccc",
                    "size": 1,
                    "snapshotId": "",
                    "availabilityZone": "us-west-2b",
                    "state": "in-use",
                    "createTime": "2014-02-27T21:43:53.0885+0000",
                    "attachments": [
                        {
                            "volumeId": "vol-ce676ccc",
                            "instanceId": "i-344c463d",
                            "device": "/dev/sdf",
                            "state": "attached",
                            "attachTime": "2014-03-07T23:46:28.0000+0000",
                            "deleteOnTermination": false
                        }
                    ],
                    "tags": [],
                    "volumeType": "standard"
                }
            }
        ],
        "configurationItemDiff": {
```

```
            "changeType": "UPDATE",
            "changedProperties": {
                "Configuration.State": {
                    "previousValue": "available",
                    "updatedValue": "in-use",
                    "changeType": "UPDATE"
                },
                "Configuration.Attachments.0": {
                    "updatedValue": {
                        "VolumeId": "vol-ce676ccc",
                        "InstanceId": "i-344c463d",
                        "Device": "/dev/sdf",
                        "State": "attached",
                        "AttachTime": "FriMar0723: 46: 28UTC2014",
                        "DeleteOnTermination": "false"
                    },
                    "changeType": "CREATE"
                }
            }
        }
    },
    "Timestamp": "2014-03-07T23:47:10.001Z",
    "SignatureVersion": "1",
    "Signature": "LgfJNB5aOk/w3omqsYrv5cUFY8yvIJvO5ZZh46/
KGPApk6HXRTBRlkhjacnxIXJEWsGI9mxvMmoWPLJGYEAR5FF/+/Ro9QTmiTNcEjQ5kB8wGsRWVrk/
whAzT2lVtofc365En2T1Ncd9iSFFXfJchgBmI7EACZ28t
+n2mWFgo57n6eGDvHTedslzC6KxkfWTfXsR6zHXzkB3XuZImktflg3iPKtvBb3Zc9iVbNsBEI4FITFWktSqqomYDjc5h0kg
+qZhMzEbHWpzFlEzvFl55KaZXxDbznBD1ZkqPgno/WufuxszCiMrsmV8pUNUnkU1TA==",
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-
e372f8ca30337fdb084e8ac449342c77.pem",
    "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:123456789012:example:a6859fee-3638-407c-907e-879651c9d143"
}
```


Item Konfigurasi untuk Sumber Daya dengan Hubungan

Jika sumber daya terkait dengan sumber daya lain, perubahan pada sumber daya tersebut dapat menghasilkan beberapa item konfigurasi. Contoh berikut menunjukkan cara AWS Config membuat item konfigurasi untuk sumber daya dengan hubungan.

1. Anda memiliki EC2 instans Amazon dengan ID`i-007d374c8912e3e90`, dan instance tersebut terkait dengan grup EC2 keamanan Amazon,`sg-c8b141b4`.

2. Anda memperbarui EC2 instans Anda untuk mengubah grup keamanan ke grup keamanan lain`sg-3f1fef43`.
3. Karena EC2 instance terkait dengan sumber daya lain, AWS Config membuat beberapa item konfigurasi seperti contoh berikut:

Pemberitahuan ini berisi perubahan item konfigurasi untuk EC2 contoh ketika grup keamanan diganti.


```
{
    "Type": "Notification",
    "MessageId": "faeba85e-ef46-570a-b01c-f8b0faae8d5d",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::EC2::Instance i-007d374c8912e3e90 Updated
 in Account 123456789012",
    "Message": {
        "configurationItemDiff": {
            "changedProperties": {
                "Configuration.NetworkInterfaces.0": {
                    "previousValue": {
                        "networkInterfaceId": "eni-fde9493f",
                        "subnetId": "subnet-2372be7b",
                        "vpcId": "vpc-14400670",
                        "description": "",
                        "ownerId": "123456789012",
                        "status": "in-use",
                        "macAddress": "0e:36:a2:2d:c5:e0",
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "sourceDestCheck": true,
                        "groups": [{
                            "groupName": "example-security-group-1",
                            "groupId": "sg-c8b141b4"
                        }],
                        "attachment": {
                            "attachmentId": "eni-attach-85bd89d9",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2017-01-09T19:36:02.000Z",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.175.43.43",
```

```
                            "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [{
                            "privateIpAddress": "172.31.16.84",
                            "privateDnsName": "ip-172-31-16-84.ec2.internal",
                            "primary": true,
                            "association": {
                                "publicIp": "54.175.43.43",
                                "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                                "ipOwnerId": "amazon"
                            }
                        }]
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                },
                "Relationships.0": {
                    "previousValue": {
                        "resourceId": "sg-c8b141b4",
                        "resourceName": null,
                        "resourceType": "AWS::EC2::SecurityGroup",
                        "name": "Is associated with SecurityGroup"
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                },
                "Configuration.NetworkInterfaces.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "networkInterfaceId": "eni-fde9493f",
                        "subnetId": "subnet-2372be7b",
                        "vpcId": "vpc-14400670",
                        "description": "",
                        "ownerId": "123456789012",
                        "status": "in-use",
                        "macAddress": "0e:36:a2:2d:c5:e0",
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "sourceDestCheck": true,
                        "groups": [{
                            "groupName": "example-security-group-2",
```

```
                            "groupId": "sg-3f1fef43"
                        }],
                        "attachment": {
                            "attachmentId": "eni-attach-85bd89d9",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2017-01-09T19:36:02.000Z",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
 "ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [{
                            "privateIpAddress": "172.31.16.84",
                            "privateDnsName": "ip-172-31-16-84.ec2.internal",
                            "primary": true,
                            "association": {
                                "publicIp": "54.175.43.43",
                                "publicDnsName":
 "ec2-54-175-43-43.compute-1.amazonaws.com",
                                "ipOwnerId": "amazon"
                            }
                        }]
                    },
                    "changeType": "CREATE"
                },
                "Relationships.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "resourceId": "sg-3f1fef43",
                        "resourceName": null,
                        "resourceType": "AWS::EC2::SecurityGroup",
                        "name": "Is associated with SecurityGroup"
                    },
                    "changeType": "CREATE"
                },
                "Configuration.SecurityGroups.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "groupName": "example-security-group-2",
                        "groupId": "sg-3f1fef43"
```

```
                    },
                    "changeType": "CREATE"
                },
                "Configuration.SecurityGroups.0": {
                    "previousValue": {
                        "groupName": "example-security-group-1",
                        "groupId": "sg-c8b141b4"
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                }
            },
            "changeType": "UPDATE"
        },
        "configurationItem": {
            "relatedEvents": [],
            "relationships": [
                {
                    "resourceId": "eni-fde9493f",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::NetworkInterface",
                    "name": "Contains NetworkInterface"
                },
                {
                    "resourceId": "sg-3f1fef43",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::SecurityGroup",
                    "name": "Is associated with SecurityGroup"
                },
                {
                    "resourceId": "subnet-2372be7b",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::Subnet",
                    "name": "Is contained in Subnet"
                },
                {
                    "resourceId": "vol-0a2d63a256bce35c5",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Is attached to Volume"
                },
                {
                    "resourceId": "vpc-14400670",
                    "resourceName": null,
```

```
                "resourceType": "AWS::EC2::VPC",
                "name": "Is contained in Vpc"
            }
        ],
        "configuration": {
            "instanceId": "i-007d374c8912e3e90",
            "imageId": "ami-9be6f38c",
            "state": {
                "code": 16,
                "name": "running"
            },
            "privateDnsName": "ip-172-31-16-84.ec2.internal",
            "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
            "stateTransitionReason": "",
            "keyName": "ec2-micro",
            "amiLaunchIndex": 0,
            "productCodes": [],
            "instanceType": "t2.micro",
            "launchTime": "2017-01-09T20:13:28.000Z",
            "placement": {
                "availabilityZone": "us-east-2c",
                "groupName": "",
                "tenancy": "default",
                "hostId": null,
                "affinity": null
            },
            "kernelId": null,
            "ramdiskId": null,
            "platform": null,
            "monitoring": {"state": "disabled"},
            "subnetId": "subnet-2372be7b",
            "vpcId": "vpc-14400670",
            "privateIpAddress": "172.31.16.84",
            "publicIpAddress": "54.175.43.43",
            "stateReason": null,
            "architecture": "x86_64",
            "rootDeviceType": "ebs",
            "rootDeviceName": "/dev/xvda",
            "blockDeviceMappings": [{
                "deviceName": "/dev/xvda",
                "ebs": {
                    "volumeId": "vol-0a2d63a256bce35c5",
                    "status": "attached",
                    "attachTime": "2017-01-09T19:36:03.000Z",
```

```
                "deleteOnTermination": true
            }
        }],
        "virtualizationType": "hvm",
        "instanceLifecycle": null,
        "spotInstanceRequestId": null,
        "clientToken": "bIYqA1483990561516",
        "tags": [{
            "key": "Name",
            "value": "value"
        }],
        "securityGroups": [{
            "groupName": "example-security-group-2",
            "groupId": "sg-3f1fef43"
        }],
        "sourceDestCheck": true,
        "hypervisor": "xen",
        "networkInterfaces": [{
            "networkInterfaceId": "eni-fde9493f",
            "subnetId": "subnet-2372be7b",
            "vpcId": "vpc-14400670",
            "description": "",
            "ownerId": "123456789012",
            "status": "in-use",
            "macAddress": "0e:36:a2:2d:c5:e0",
            "privateIpAddress": "172.31.16.84",
            "privateDnsName": "ip-172-31-16-84.ec2.internal",
            "sourceDestCheck": true,
            "groups": [{
                "groupName": "example-security-group-2",
                "groupId": "sg-3f1fef43"
            }],
            "attachment": {
                "attachmentId": "eni-attach-85bd89d9",
                "deviceIndex": 0,
                "status": "attached",
                "attachTime": "2017-01-09T19:36:02.000Z",
                "deleteOnTermination": true
            },
            "association": {
                "publicIp": "54.175.43.43",
                "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
                "ipOwnerId": "amazon"
            },
```

```
                    "privateIpAddresses": [{
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "primary": true,
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
 "ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        }
                    }]
                }],
                "iamInstanceProfile": null,
                "ebsOptimized": false,
                "sriovNetSupport": null,
                "enaSupport": true
            },
            "supplementaryConfiguration": {},
            "tags": {"Name": "value"},
            "configurationItemVersion": "1.2",
            "configurationItemCaptureTime": "2017-01-09T22:50:14.328Z",
            "configurationStateId": 1484002214328,
            "awsAccountId": "123456789012",
            "configurationItemStatus": "OK",
            "resourceType": "AWS::EC2::Instance",
            "resourceId": "i-007d374c8912e3e90",
            "resourceName": null,
            "ARN": "arn:aws:ec2:us-east-2:123456789012:instance/i-007d374c8912e3e90",
            "awsRegion": "us-east-2",
            "availabilityZone": "us-east-2c",
            "configurationStateMd5Hash": "8d0f41750f5965e0071ae9be063ba306",
            "resourceCreationTime": "2017-01-09T20:13:28.000Z"
        },
        "notificationCreationTime": "2017-01-09T22:50:15.928Z",
        "messageType": "ConfigurationItemChangeNotification",
        "recordVersion": "1.2"
    },
    "Timestamp": "2017-01-09T22:50:16.358Z",
    "SignatureVersion": "1",
    "Signature": "lpJTEYOSr8fUbiaaRNw1ECawJFVoD7I67mIeEkfAWJkqvvpak1ULHLlC
+I0sS/01A4P1Yci8GSK/cOEC/O2XBntlw4CAtbMUgTQvb345Z2YZwcpK0kPNi6v6N51DuZ/6DZA8EC
+gVTNTO09xtNIH8aMlvqyvUSXuh278xayExC5yTRXEg+ikdZRd4QzS7obSK1kgRZWI6ipxPNL6rd56/
VvPxyhcbS7Vm40/2+e0nVb3bjNHBxjQTXSs1Xhuc9eP2gEsC4Sl32bGqdeDU1Y4dFGukuzPYoHuEtDPh
+GkLUq3KeiDAQshxAZLmOIRcQ7iJ/bELDJTN9AcX6lqlDZ79w==",
```

```
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

Pemberitahuan ini berisi perubahan item konfigurasi untuk grup EC2 keamanan`sg-3f1fef43`, yang terkait dengan instance.

```
{
    "Type": "Notification",
    "MessageId": "564d873e-711e-51a3-b48c-d7d064f65bf4",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::EC2::SecurityGroup sg-3f1fef43 Created in
 Account 123456789012",
    "Message": {
        "configurationItemDiff": {
            "changedProperties": {},
            "changeType": "CREATE"
        },
        "configurationItem": {
            "relatedEvents": [],
            "relationships": [{
                "resourceId": "vpc-14400670",
                "resourceName": null,
                "resourceType": "AWS::EC2::VPC",
                "name": "Is contained in Vpc"
            }],
            "configuration": {
                "ownerId": "123456789012",
                "groupName": "example-security-group-2",
                "groupId": "sg-3f1fef43",
                "description": "This is an example security group.",
                "ipPermissions": [],
                "ipPermissionsEgress": [{
                    "ipProtocol": "-1",
                    "fromPort": null,
                    "toPort": null,
                    "userIdGroupPairs": [],
                    "ipRanges": ["0.0.0.0/0"],
                    "prefixListIds": []
                }],
```

```
                "vpcId": "vpc-14400670",
                "tags": []
            },
            "supplementaryConfiguration": {},
            "tags": {},
            "configurationItemVersion": "1.2",
            "configurationItemCaptureTime": "2017-01-09T22:50:15.156Z",
            "configurationStateId": 1484002215156,
            "awsAccountId": "123456789012",
            "configurationItemStatus": "ResourceDiscovered",
            "resourceType": "AWS::EC2::SecurityGroup",
            "resourceId": "sg-3f1fef43",
            "resourceName": null,
            "ARN": "arn:aws:ec2:us-east-2:123456789012:security-group/sg-3f1fef43",
            "awsRegion": "us-east-2",
            "availabilityZone": "Not Applicable",
            "configurationStateMd5Hash": "7399608745296f67f7fe1c9ca56d5205",
            "resourceCreationTime": null
        },
        "notificationCreationTime": "2017-01-09T22:50:16.021Z",
        "messageType": "ConfigurationItemChangeNotification",
        "recordVersion": "1.2"
    },
    "Timestamp": "2017-01-09T22:50:16.413Z",
    "SignatureVersion": "1",
    "Signature": "GocX31Uu/zNFo85hZqzsNy30skwmLnjPjj+UjaJzkih
+dCP6gXYGQ0bK7uMzaLL2C/ibYOOsT7I/XY4NW6Amc5T46ydyHDjFRtQi8UfUQTqLXYRTnpOO/
hyK9lMFfhUNs4NwQpmx3n3mYEMpLuMs8DCgeBmB3AQ+hXPhNuNuR3mJVgo25S8AqphN9O0okZ2MKNUQy8iJm/
CVAx70TdnYsfUMZ24n88bUzAfiHGzc8QTthMdrFVUwXxa1h/7Zl8+A7BwoGmjo7W8CfLDVwaIQv1Uplgk3qd95Z0AXOzXVx
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Memahami **configurationItemDiff** bidang di notifikasi Amazon SNS **ConfigurationItemChangeNotification**

AWS Config membuat item konfigurasi setiap kali konfigurasi sumber daya berubah (create/update/delete). Untuk daftar jenis sumber daya yang didukung yang AWS Config dapat merekam, lihat[Jenis Sumber Daya yang Didukung untuk AWS Config]. AWS Config menggunakan Amazon SNS untuk

mengirimkan pemberitahuan saat perubahan terjadi. Payload notifikasi Amazon SNS menyertakan bidang untuk membantu Anda melacak perubahan sumber daya di Wilayah tertentu. AWS

Untuk memahami mengapa Anda menerima `ConfigurationItemChangeNotification` pemberitahuan, tinjau `configurationItemDiff` detailnya. Bidang bervariasi tergantung pada jenis perubahan dan dapat membentuk kombinasi yang berbeda seperti UPDATE-UPDATE, UPDATE-CREATE, dan DELETE-DELETE. Berikut ini adalah penjelasan dari beberapa kombinasi umum.

UPDATE-CREATE dan UPDATE-UPDATE

Contoh berikut mencakup perubahan dalam hubungan langsung sumber daya dan konfigurasi sumber daya. `configurationItemDiff`Detailnya mengungkapkan informasi berikut:

Tindakan yang dilakukan: Kebijakan terkelola yang ada di akun dilampirkan ke peran AWS Identity and Access Management (IAM).

Operasi dasar dilakukan: UPDATE (memperbarui jumlah asosiasi jenis sumber daya `AWS::IAM::Policy` dalam akun).

Ubah kombinasi tipe:

1. Perubahan hubungan langsung sumber daya UPDATE-CREATE. Lampiran atau asosiasi baru dibuat antara kebijakan IAM dan peran IAM.
2. Perubahan konfigurasi sumber daya UPDATE-UPDATE. Jumlah asosiasi kebijakan IAM meningkat dari 2 menjadi 3 ketika kebijakan dilampirkan pada peran IAM.

Contoh pemberitahuan UPDATE-CREATE dan UPDATE-UPDATE: `configurationItemDiff`

```
{
    "configurationItemDiff": {
        "changedProperties": {
            "Relationships.0": {
                "previousValue": null,
                "updatedValue": {
                    "resourceId": "AROA6D3M4S53*********",
                    "resourceName": "Test1",
                    "resourceType": "AWS::IAM::Role",
                    "name": "Is attached to Role"
                },
                "changeType": "CREATE"                 >>>>>>>>>>>>>>>>>>>>> 1
            },
```

```
            "Configuration.AttachmentCount": {
                "previousValue": 2,
                "updatedValue": 3,
                "changeType": "UPDATE"                >>>>>>>>>>>>>>>>>>>> 2
            }
        },
        "changeType": "UPDATE"
    }
}
```

PEMBARUAN-HAPUS

Contoh berikut mencakup perubahan dalam hubungan langsung sumber daya dan konfigurasi sumber daya. `configurationItemDiff`Detailnya mengungkapkan informasi berikut:

Tindakan dilakukan: Kebijakan terkelola yang ada di akun terlepas dari pengguna IAM.

Operasi dasar dilakukan: UPDATE (memperbarui kebijakan izin yang terkait dengan jenis sumber daya`AWS::IAM::User`).

Ubah kombinasi tipe: Perubahan hubungan langsung sumber daya UPDATE-DELETE. Hubungan antara pengguna IAM dan kebijakan IAM di akun telah dihapus.

Contoh pemberitahuan UPDATE-DELETE`configurationItemDiff`:

JSON

```
{
  "configurationItemDiff": {
    "changedProperties": {
      "Configuration.UserPolicyList.0": {
        "previousValue": {
          "policyName": "Test2",
          "policyDocument": "{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "StringLike": {
```

```
                    "aws:RequestTag/VPCId": "*"
                }
            }
        }
    ]
}"
        },
        "updatedValue": null,
        "changeType": "DELETE"                        >>>>>>>>>>>>>>>>>>>> 3
      }
    },
    "changeType": "UPDATE"
  }
}
```

HAPUS-HAPUS

Contoh berikut mencakup perubahan dalam hubungan langsung sumber daya dan konfigurasi sumber daya. `configurationItemDiff`Detailnya mengungkapkan informasi berikut:

Tindakan yang dilakukan: Peran IAM yang ada di akun telah dihapus.

Operasi dasar dilakukan: DELETE (sumber daya dari jenis sumber daya `AWS::IAM::Role` dihapus).

Ubah kombinasi tipe: Perubahan hubungan langsung sumber daya dan perubahan konfigurasi sumber daya DELETE-DELETE. Penghapusan peran IAM juga menghapus asosiasi kebijakan IAM dengan peran IAM.

Contoh pemberitahuan HAPUS-HAPUS`configurationItemDiff`:

JSON

```
{
  "configurationItemDiff": {
    "changedProperties": {
      "Relationships.0": {
        "previousValue": {
          "resourceId": "ANPAIJ5MXUKK*********",
          "resourceName": "AWSCloudTrailAccessPolicy",
          "resourceType": "AWS::IAM::Policy",
          "name": "Is attached to CustomerManagedPolicy"
```

```
        },
        "updatedValue": null,
        "changeType": "DELETE"
      },
      "Configuration": {
        "previousValue": {
          "path": "/",
          "roleName": "CloudTrailRole",
          "roleId": "AROAJITJ6YGM*********",
          "arn": "arn:aws:iam::123456789012:role/CloudTrailRole",
          "createDate": "2017-12-06T10:27:51.000Z",
          "assumeRolePolicyDocument": "{"Version":"2012-10-17","Statement":
[{"Sid":"","Effect":"Allow","Principal":
{"AWS":"arn:aws:iam::123456789012:root"},"Action":"sts:AssumeRole","Condition":
{"StringEquals":{"sts:ExternalId":"123456"}}}]}",
          "instanceProfileList": [],
          "rolePolicyList": [],
          "attachedManagedPolicies": [
            {
              "policyName": "AWSCloudTrailAccessPolicy",
              "policyArn": "arn:aws:iam::123456789012:policy/
AWSCloudTrailAccessPolicy"
            }
          ],
          "permissionsBoundary": null,
          "tags": [],
          "roleLastUsed": null
        },
        "updatedValue": null,
        "changeType": "DELETE"
      }
    },
    "changeType": "DELETE"
}
```

Contoh Pemberitahuan Pengiriman Riwayat Konfigurasi

Riwayat konfigurasi adalah kumpulan item konfigurasi untuk jenis sumber daya selama periode waktu. Berikut ini adalah contoh pemberitahuan yang AWS Config mengirimkan ketika riwayat konfigurasi untuk sumber daya CloudTrail jejak dikirimkan untuk akun Anda.

```
{
```

```
    "Type": "Notification",
    "MessageId": "ce49bf2c-d03a-51b0-8b6a-ef480a8b39fe",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration History Delivery Completed for
 Account 123456789012",
    "Message": {
        "s3ObjectKey": "AWSLogs/123456789012/Config/us-east-2/2016/9/27/
ConfigHistory/123456789012_Config_us-
east-2_ConfigHistory_AWS::CloudTrail::Trail_20160927T195818Z_20160927T195818Z_1.json.gz",
        "s3Bucket": "config-bucket-123456789012-ohio",
        "notificationCreationTime": "2016-09-27T20:37:05.217Z",
        "messageType": "ConfigurationHistoryDeliveryCompleted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-09-27T20:37:05.315Z",
    "SignatureVersion": "1",
    "Signature": "OuIcS5RAKXTR6chQEJp3if4KJQVlBz2kmXh7QE1/
RJQiCPsCNfG0J0rUZ1rqfKMqpps/Ka+zF0kg4dUCWV9PF0dliuwnjfbtYmDZpP4EBOoGmxcTliUn1AIe/
yeGFDuc6P3EotP3zt02rhmxjezjf3c11urstFZ8rTLVXp0z0xeyk4da0UetLsWZxUFEG0Z5uhk09mBo5dg/4mryIOovidhr
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Contoh Konfigurasi Pengiriman Snapshot Mulai Pemberitahuan

Berikut ini adalah contoh pemberitahuan yang AWS Config mengirim ketika AWS Config mulai mengirimkan snapshot konfigurasi untuk akun Anda.


```
{
    "Type": "Notification",
    "MessageId": "a32d0487-94b1-53f6-b4e6-5407c9c00be6",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration Snapshot Delivery Started for
 Account 123456789012",
    "Message": {
        "configSnapshotId": "108e0794-84a7-4cca-a179-76a199ddd11a",
        "notificationCreationTime": "2016-10-18T17:26:09.572Z",
        "messageType": "ConfigurationSnapshotDeliveryStarted",
        "recordVersion": "1.1"
    },
```

```
    "Timestamp": "2016-10-18T17:26:09.840Z",
    "SignatureVersion": "1",
    "Signature": "BBA0DeKsfteTpYyZH5HPANpOLmW/jumOMBsghRq/kimY9tjNlkF/
V3BpLG1HVmDQdQzBh6oKE0h0rxcazbyGf5KF5W5r1zKKlEnS9xugFzALPUx//
olSJ4neWalLBKNIq1xvAQgu9qHfDR7dS2aCwe4scQfqOjn1Ev7PlZqxmT+ux3SR/
C54cbfcduDpDsPwdo868+TpZvMtaU30ySnX04fmOgxoiA8AJO/EnjduQ08/zd4SYXhm
+H9wavcwXB9XECelHhRW70Y+wHQixfx40S1SaSRzvnJE+m9mHphFQs64YraRDRv6tMaenTk6CVPO
+81ceAXIg2E1m7hZ7lz4PA==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Contoh Konfigurasi Pemberitahuan Pengiriman Snapshot

Snapshot konfigurasi adalah kumpulan item konfigurasi untuk semua sumber daya yang direkam dan konfigurasinya di akun Anda. Berikut ini adalah contoh pemberitahuan yang AWS Config mengirim ketika snapshot konfigurasi dikirimkan untuk akun Anda.


```
{
    "Type": "Notification",
    "MessageId": "9fc82f4b-397e-5b69-8f55-7f2f86527100",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration Snapshot Delivery Completed for
 Account 123456789012",
    "Message": {
        "configSnapshotId": "16da64e4-cb65-4846-b061-e6c3ba43cb96",
        "s3ObjectKey": "AWSLogs/123456789012/Config/us-east-2/2016/9/27/
ConfigSnapshot/123456789012_Config_us-east-2_ConfigSnapshot_20160927T183939Z_16da64e4-
cb65-4846-b061-e6c3ba43cb96.json.gz",
        "s3Bucket": "config-bucket-123456789012-ohio",
        "notificationCreationTime": "2016-09-27T18:39:39.853Z",
        "messageType": "ConfigurationSnapshotDeliveryCompleted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-09-27T18:39:40.062Z",
    "SignatureVersion": "1",
    "Signature": "PMkWfUuj/fKIEXA7s2wTDLbZoF/MDsUkPspYghOpwu9n6m+C
+zrm0cEZXPxxJPvhnWozG7SVqkHYf9QgI/diW2twP/HPDn5GQs2rNDc+YlaByEXnKVtHV1Gd4r1kN57E/
oOW5NVLNczk5ymxAW+WGdptZJkCgyVuhJ28s08m3Z3Kqz96PPSnXzYZoCfCn/
yP6CqXoN7olr4YCbYxYwn8zOUYcPmc45yYNSUTKZi+RJQRnDJkL2qb
```

```
+s4h9w2fjbBBj8xe830VbFJqbHp7UkSfpc64Y+tRvmMLY5CI1cYrnuPRhTLdUk+R0sshg5G+JMtSLVG/
TvWbjz44CKXJprjIQg==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

Contoh Pemberitahuan Perubahan Kepatuhan

Saat AWS Config mengevaluasi sumber daya Anda terhadap aturan khusus atau terkelola, AWS Config kirimkan pemberitahuan yang menunjukkan apakah sumber daya sesuai dengan aturan tersebut.

Berikut ini adalah contoh pemberitahuan di mana sumber daya CloudTrail jejak sesuai dengan aturan yang `cloudtrail-enabled` dikelola.

```
{
    "Type": "Notification",
    "MessageId": "11fd05dd-47e1-5523-bc01-55b988bb9478",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::::Account 123456789012 is COMPLIANT with
 cloudtrail-enabled in Accoun...",
    "Message": {
        "awsAccountId": "123456789012",
        "configRuleName": "cloudtrail-enabled",
        "configRuleARN": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-9rpvxc",
        "resourceType": "AWS::::Account",
        "resourceId": "123456789012",
        "awsRegion": "us-east-2",
        "newEvaluationResult": {
            "evaluationResultIdentifier": {
                "evaluationResultQualifier": {
                    "configRuleName": "cloudtrail-enabled",
                    "resourceType": "AWS::::Account",
                    "resourceId": "123456789012"
                },
                "orderingTimestamp": "2016-09-27T19:48:40.619Z"
            },
            "complianceType": "COMPLIANT",
            "resultRecordedTime": "2016-09-27T19:48:41.405Z",
```

```
            "configRuleInvokedTime": "2016-09-27T19:48:40.914Z",
            "annotation": null,
            "resultToken": null
        },
        "oldEvaluationResult": {
            "evaluationResultIdentifier": {
                "evaluationResultQualifier": {
                    "configRuleName": "cloudtrail-enabled",
                    "resourceType": "AWS::::Account",
                    "resourceId": "123456789012"
                },
                "orderingTimestamp": "2016-09-27T16:30:49.531Z"
            },
            "complianceType": "NON_COMPLIANT",
            "resultRecordedTime": "2016-09-27T16:30:50.717Z",
            "configRuleInvokedTime": "2016-09-27T16:30:50.105Z",
            "annotation": null,
            "resultToken": null
        },
        "notificationCreationTime": "2016-09-27T19:48:42.620Z",
        "messageType": "ComplianceChangeNotification",
        "recordVersion": "1.0"
    },
    "Timestamp": "2016-09-27T19:48:42.749Z",
    "SignatureVersion": "1",
    "Signature": "XZ9FfLb2ywkW9yj0yBkNtIP5q7Cry6JtCEyUiHmG9gpOZi3seQ41udhtAqCZoiNiizAEi
+6gcttHCRV1hNemzp/
YmBmTfO6azYXt0FJDaEvd86k68VCS9aqRlBBjYlNo7ILi4Pqd5rE4BX2YBQSzcQyERGkUfTZ2BIFyAmb1Q/
y4/6ez8rDyi545FDSlgcGEb4LKLNR6eDi4FbKtMGZHA7Nz8obqs1dHbgWYnp3c80mVLl7ohP4hilcxdywAgXrbsN32ekYr1
+BIZ21ZtkcUtY5B3ImgRlUO7Yhn3L3c6rZxQ==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Contoh: Perubahan Item Konfigurasi Konfigurasi | Amazon EventBridge


```
{
  "version": "0",
  "id": "00bdf13e-1111-b2f5-cef0-e9cbbe7cd533",
  "detail-type": "Config Configuration Item Change",
```

```
  "source": "aws.config",
  "account": "123456789012",
  "time": "2022-03-16T01:10:51Z",
  "region": "us-east-1",
  "resources": ["arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95"],
  "detail": {
    "recordVersion": "1.3",
    "messageType": "ConfigurationItemChangeNotification",
    "configurationItemDiff": {
      "changedProperties": {
        "Configuration.FileSystemTags.0": {
          "updatedValue": {
            "Key": "test",
            "Value": "me"
          },
          "changeType": "CREATE"
        },
        "Tags.2": {
          "updatedValue": "me",
          "changeType": "CREATE"
        }
      },
      "changeType": "UPDATE"
    },
    "notificationCreationTime": "2022-03-16T01:10:51.976Z",
    "configurationItem": {
      "relatedEvents": [],
      "relationships": [],
      "configuration": {
        "FileSystemId": "fs-01f0d526165b57f95",
        "Arn": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95",
        "Encrypted": true,
        "FileSystemTags": [{
          "Key": "Name",
          "Value": "myname"
        }, {
          "Key": "test",
          "Value": "me"
        }],
        "PerformanceMode": "generalPurpose",
        "ThroughputMode": "bursting",
        "LifecyclePolicies": [{
```

```
          "TransitionToIA": "AFTER_30_DAYS"
        }, {
          "TransitionToPrimaryStorageClass": "AFTER_1_ACCESS"
        }],
        "BackupPolicy": {
          "Status": "ENABLED"
        },
        "FileSystemPolicy": {},
        "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/0e6c91d5-e23b-4ed3-
bd36-1561fbbc0a2d"
      },
      "supplementaryConfiguration": {},
      "tags": {
        "aws:elasticfilesystem:default-backup": "enabled",
        "test": "me",
        "Name": "cloudcontroltest1"
      },
      "configurationItemVersion": "1.3",
      "configurationItemCaptureTime": "2022-03-16T01:10:50.837Z",
      "configurationStateId": 1647393050837,
      "awsAccountId": "123456789012",
      "configurationItemStatus": "OK",
      "resourceType": "AWS::EFS::FileSystem",
      "resourceId": "fs-01f0d526165b57f95",
      "resourceName": "fs-01f0d526165b57f95",
      "ARN": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95",
      "awsRegion": "us-east-1",
      "availabilityZone": "Regional",
      "configurationStateMd5Hash": ""
    }
  }
}
```

Contoh Aturan Evaluasi Mulai Pemberitahuan

AWS Config mengirimkan pemberitahuan saat mulai mengevaluasi aturan kustom atau terkelola terhadap sumber daya Anda. Berikut ini adalah contoh pemberitahuan ketika AWS Config mulai mengevaluasi aturan yang `iam-password-policy` dikelola.

```
{
    "Type": "Notification",
    "MessageId": "358c8e65-e27a-594e-82d0-de1fe77393d7",
```

```
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Config Rules Evaluation Started for Account
 123456789012",
    "Message": {
        "awsAccountId": "123456789012",
        "awsRegion": "us-east-2",
        "configRuleNames": ["iam-password-policy"],
        "notificationCreationTime": "2016-10-13T21:55:21.339Z",
        "messageType": "ConfigRulesEvaluationStarted",
        "recordVersion": "1.0"
    },
    "Timestamp": "2016-10-13T21:55:21.575Z",
    "SignatureVersion": "1",
    "Signature": "DE431D+24zzFRboyPY2bPTsznJWe8L6TjDC+ItYlLFkE9jACSBl3sQ1uSjYzEhEbN7Cs
+wBoHnJ/DxOSpyCxt4giqgKd+H2I636BvrQwHDhJwJm7qI6P8IozEliRvRWbM38zDTvHqkmmXQbdDHRsK/
MssMeVTBKuW0x8ivMrj+KpwuF57tE62eXeFhjBeJ0DKQV+aC+i3onsuT7HQvXQDBPdOM
+cSuLrJaMQJ6TcMU5G76qg/
gl494ilb4Vj4udboGWpHSgUvI3guFsc1SsTrlWXQKXabWtsCQPfdOhkKgmViCfMZrLRp8Pjnu
+uspYQELkEfwBchDVVzd15iMrAzQ==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Contoh Pemberitahuan Perubahan Item Konfigurasi Besar

Ketika AWS Config mendeteksi perubahan konfigurasi untuk sumber daya, ia mengirimkan pemberitahuan item konfigurasi (CI). Jika notifikasi melebihi ukuran maksimum yang diizinkan oleh Amazon Simple Notification Service (Amazon SNS), notifikasi tersebut menyertakan ringkasan singkat item konfigurasi.

Anda dapat melihat notifikasi lengkap di lokasi bucket Amazon S3 yang ditentukan di bidang. `s3BucketLocation`

Contoh pemberitahuan berikut menunjukkan CI untuk EC2 instance Amazon. Pemberitahuan tersebut mencakup ringkasan perubahan dan lokasi notifikasi di bucket Amazon S3.

```
View the Timeline for this Resource in the Console:
```

```
    https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/
AWS::EC2::Instance/resourceId_14b76876-7969-4097-ab8e-a31942b02e80?
time=2016-10-06T16:46:16.261Z

    The full configuration item change notification for this resource exceeded the
 maximum size allowed by Amazon Simple Notification Service (SNS). A summary of the
 configuration item is provided here. You can view the complete notification in the
 specified Amazon S3 bucket location.

    New State Record Summary:
    ----------------------------
    {
      "configurationItemSummary": {
        "changeType": "UPDATE",
        "configurationItemVersion": "1.2",
        "configurationItemCaptureTime": "2016-10-06T16:46:16.261Z",
        "configurationStateId": 0,
        "awsAccountId": "123456789012",
        "configurationItemStatus": "OK",
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/
resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
        "awsRegion": "us-west-2",
        "availabilityZone": null,
        "configurationStateMd5Hash": "8f1ee69b287895a0f8bc5753eca68e96",
        "resourceCreationTime": "2016-10-06T16:46:10.489Z"
      },
      "s3DeliverySummary": {
        "s3BucketLocation": "amzn-s3-demo-bucket/AWSLogs/123456789012/
Config/us-west-2/2016/10/6/OversizedChangeNotification/AWS::EC2::Instance/
resourceId_14b76876-7969-4097-ab8e-a31942b02e80/123456789012_Config_us-
west-2_ChangeNotification_AWS::EC2::Instance_resourceId_14b76876-7969-4097-ab8e-
a31942b02e80_20161006T164616Z_0.json.gz",
        "errorCode": null,
        "errorMessage": null
      },
      "notificationCreationTime": "2016-10-06T16:46:16.261Z",
      "messageType": "OversizedConfigurationItemChangeNotification",
      "recordVersion": "1.0"
    }
```

Cara mengakses item konfigurasi besar

Saat item konfigurasi terlalu besar, hanya ringkasan yang dikirim ke Amazon SNS. Item konfigurasi lengkap (CI) disimpan di Amazon S3

Contoh kode berikut menunjukkan cara mengakses CI lengkap.

```
import boto3
import json

def handle_oversized_configuration_item(event):
    """
    Example of handling an oversized configuration item notification

    When a configuration item is oversized:
    1. AWS Config sends a summary notification through SNS
    2. The complete configuration item is stored in S3
    3. Use get_resource_config_history API to retrieve the complete configuration
    """

    # Extract information from the summary notification
    if event['messageType'] == 'OversizedConfigurationItemChangeNotification':
        summary = event['configurationItemSummary']
        resource_type = summary['resourceType']
        resource_id = summary['resourceId']

        # Initialize AWS Config client
        config_client = boto3.client('config')

        # Retrieve the complete configuration item
        response = config_client.get_resource_config_history(
            resourceType=resource_type,
            resourceId=resource_id
        )

        if response['configurationItems']:
            config_item = response['configurationItems'][0]

            # For EC2 instances, the configuration contains instance details
            configuration = json.loads(config_item['configuration'])
            print(f"Instance Configuration: {configuration}")

            # Handle supplementary configuration if present
```

```
            if 'supplementaryConfiguration' in config_item:
                for key, value in config_item['supplementaryConfiguration'].items():
                    if isinstance(value, str):
                        config_item['supplementaryConfiguration'][key] =
 json.loads(value)
                print(f"Supplementary Configuration:
 {config_item['supplementaryConfiguration']}")

            return config_item

        # If needed, you can also access the complete notification from S3
        s3_location = event['s3DeliverySummary']['s3BucketLocation']
        print(f"Complete notification available in S3: {s3_location}")

    return None
```

Cara kerjanya

1. Fungsi menerima parameter peristiwa yang berisi AWS Config notifikasi.
2. Ini memeriksa apakah jenis pesan adalah pemberitahuan konfigurasi yang terlalu besar.
3. Fungsi mengekstrak jenis sumber daya dan ID dari ringkasan.
4. Menggunakan AWS Config klien, ia mengambil riwayat konfigurasi lengkap.
5. Fungsi ini memproses konfigurasi utama dan tambahan.
6. Jika diperlukan, Anda dapat mengakses notifikasi lengkap dari lokasi S3 yang disediakan.

Contoh Pemberitahuan Gagal Pengiriman

AWS Config mengirimkan pemberitahuan gagal pengiriman jika tidak AWS Config dapat mengirimkan snapshot konfigurasi atau pemberitahuan perubahan item konfigurasi berukuran besar ke bucket Amazon S3 Anda. Pastikan Anda menetapkan bucket Amazon S3 yang valid.

```
View the Timeline for this Resource in the Console:
    https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/
AWS::EC2::Instance/test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457?
time=2016-10-06T16:46:13.749Z

     The full configuration item change notification for this resource exceeded the
 maximum size allowed by Amazon Simple Notification Service (SNS). A summary of the
 configuration item is provided here. You can view the complete notification in the
 specified Amazon S3 bucket location.
```

```
    New State Record Summary:
    ----------------------------
    {
      "configurationItemSummary": {
        "changeType": "UPDATE",
        "configurationItemVersion": "1.2",
        "configurationItemCaptureTime": "2016-10-06T16:46:13.749Z",
        "configurationStateId": 0,
        "awsAccountId": "123456789012",
        "configurationItemStatus": "OK",
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/
test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
        "awsRegion": "us-west-2",
        "availabilityZone": null,
        "configurationStateMd5Hash": "6de64b95eacd30e7b63d4bba7cd80814",
        "resourceCreationTime": "2016-10-06T16:46:10.489Z"
      },
      "s3DeliverySummary": {
        "s3BucketLocation": null,
        "errorCode": "NoSuchBucket",
        "errorMessage": "Failed to deliver notification to bucket: bucket-example for
 account 123456789012 in region us-west-2."
      },
      "notificationCreationTime": "2016-10-06T16:46:13.749Z",
      "messageType": "OversizedConfigurationItemChangeDeliveryFailed",
      "recordVersion": "1.0"
    }
```

Melihat AWS Config Dasbor

Gunakan Dasbor untuk melihat ikhtisar sumber daya, aturan, paket kesesuaian, dan status kepatuhannya serta untuk memvisualisasikan metrik AWS Config penggunaan dan keberhasilan Anda dengan Amazon. CloudWatch Halaman ini membantu Anda dengan cepat mengidentifikasi sumber daya teratas di AWS akun Anda, paket kesesuaian dengan tingkat kepatuhan terendah, aturan atau sumber daya apa yang tidak sesuai dengan Anda Akun AWS, lalu lintas apa yang mendorong AWS Config penggunaan Anda Akun AWS, dan metrik kunci untuk keberhasilan dan kegagalan yang telah terjadi dalam alur kerja Anda.

Untuk menggunakan AWS Config Dashboard

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Di panel navigasi kiri, pilih Dasbor.

Daftar Isi

- Kepatuhan dan Inventarisasi Sumber Daya
- AWS Config Metrik Penggunaan dan Sukses

Kepatuhan dan Inventarisasi Sumber Daya

Setelah penyiapan, AWS Config mulailah merekam sumber daya yang Anda tentukan dan evaluasi terhadap aturan Anda. Mungkin perlu beberapa menit AWS Config untuk menampilkan sumber daya, aturan, paket kesesuaian, dan status kepatuhan Anda.

Paket kesesuaian berdasarkan skor kepatuhan

Paket kesesuaian berdasarkan skor kepatuhan menampilkan hingga 10 paket kesesuaian Anda dengan skor kepatuhan terendah. Skor kepatuhan adalah persentase dari jumlah kombinasi aturan-sumber daya yang sesuai dalam paket kesesuaian dibandingkan dengan jumlah total kemungkinan kombinasi aturan-sumber daya dalam paket kesesuaian.

Metrik ini memberi Anda pandangan tingkat tinggi tentang status kepatuhan paket kesesuaian Anda, dan dapat digunakan untuk mengidentifikasi, menyelidiki, dan memahami tingkat kepatuhan dalam paket kesesuaian Anda. Anda dapat menggunakan skor kepatuhan untuk

melacak kemajuan remediasi, melakukan perbandingan di berbagai rangkaian persyaratan, dan melihat dampak perubahan atau penerapan tertentu terhadap paket kesesuaian.

Untuk melihat status penerapan, skor kepatuhan, garis waktu skor kepatuhan, dan aturan untuk paket kesesuaian dalam tampilan mendetail, pilih nama paket kesesuaian di bawah Paket kesesuaian.

Status kepatuhan

Status kepatuhan menampilkan jumlah aturan yang sesuai dan tidak patuh serta sumber daya yang sesuai dan tidak patuh. Sumber daya sesuai atau tidak sesuai berdasarkan evaluasi aturan yang terkait dengannya. Jika sumber daya tidak mengikuti spesifikasi aturan, sumber daya dan aturan ditandai sebagai tidak sesuai.

Untuk melihat daftar aturan dan sumber daya yang tidak sesuai, pilih Aturan yang tidak sesuai atau Sumber daya yang tidak sesuai.

Aturan oleh sumber daya yang tidak patuh

Aturan berdasarkan sumber daya yang tidak sesuai menampilkan aturan tidak patuh teratas Anda dalam urutan menurun menurut jumlah sumber daya. Pilih aturan untuk melihat detail, parameter, dan sumber daya dalam cakupan aturan khusus itu.

Untuk daftar lengkap aturan yang tidak patuh, pilih Lihat semua aturan yang tidak patuh.

Persediaan sumber daya

Inventaris sumber daya menampilkan jumlah total sumber daya AWS Config yang direkam dalam urutan menurun dengan jumlah sumber daya, dan jumlah setiap jenis sumber daya di sumber daya Anda Akun AWS. Untuk membuka semua sumber daya untuk jenis sumber daya, pilih jenis sumber daya tersebut untuk membuka halaman inventaris Resources.

Anda dapat menggunakan daftar dropdown untuk menunjukkan total sumber daya yang ingin Anda lihat. Secara default, ini diatur untuk melihat Semua sumber daya, tetapi Anda dapat mengubahnya menjadi AWS sumber daya, sumber daya pihak ketiga, atau Sumber daya khusus.

> **Note**
>
> Pesan Evaluasi konfigurasi AWS sumber daya Anda menggunakan aturan Config dapat muncul di Dasbor karena alasan berikut:

- Anda belum mengatur AWS Config aturan untuk Anda Akun AWS. Anda dapat memilih Tambahkan aturan untuk pergi ke halaman Aturan.
- AWS Config masih mengevaluasi sumber daya Anda terhadap aturan Anda. Anda dapat me-refresh halaman untuk melihat hasil evaluasi terbaru.
- AWS Config mengevaluasi sumber daya Anda terhadap aturan Anda dan tidak menemukan sumber daya apa pun dalam ruang lingkup. Anda dapat menentukan sumber daya AWS Config untuk direkam di halaman Pengaturan. Untuk informasi selengkapnya, lihat Merekam AWS Sumber Daya dengan AWS Config.

AWS Config Metrik Penggunaan dan Sukses

Anda dapat menggunakan CloudWatch dasbor Amazon di AWS Config konsol untuk memvisualisasikan metrik AWS Config penggunaan dan keberhasilan Anda.

Untuk setiap dasbor, Anda dapat melakukan hal berikut:

- Sesuaikan rentang waktu dasbor untuk menampilkan data dari 3 Jam, 1 Hari, atau 1 Minggu terakhir.
- Pilih ikon Kalender, untuk memasukkan rentang waktu khusus: baik waktu Relatif untuk jumlah waktu yang ditentukan sebelumnya atau rentang waktu Absolut antara dua tanggal.
- Anda dapat mengubah format waktu untuk menampilkan data dasbor di UTC (Waktu Universal Terkoordinasi) atau zona waktu lokal (zona waktu yang ditentukan sebagai zona waktu lokal Anda di sistem operasi perangkat Anda).
- Gunakan panah Jatuhkan di sebelah ikon Refresh untuk menentukan seberapa sering data di dasbor harus disegarkan, atau untuk mematikan penyegaran otomatis. Pilih Mati, 10 Detik, 1 Menit, 2 Menit, 5 Menit, atau 15 Menit untuk mengubah internal penyegaran.
- Pilih Opsi lainnya (menu elipsis vertikal) untuk menambahkan metrik AWS Config penggunaan atau metrik AWS Config keberhasilan yang sedang Anda lihat di AWS Config Dasbor ke konsol. CloudWatch Ini membuka tab baru di CloudWatch konsol yang memungkinkan Anda membuat dasbor khusus baru CloudWatch dengan informasi yang disalin dari metrik AWS Config penggunaan atau metrik AWS Config keberhasilan Anda saat ini.

Jika Anda ingin melakukan analisis tambahan terhadap metrik ini CloudWatch, pilih Metrik di panel navigasi kiri CloudWatch konsol, lalu pilih /Config.AWS Untuk informasi selengkapnya tentang hal

yang dapat Anda lakukan dari CloudWatch konsol, lihat Menggunakan CloudWatch dasbor Amazon dan Menggunakan CloudWatch metrik Amazon di CloudWatch Panduan Pengguna.

AWS Config Metrik Penggunaan

Metrik	Deskripsi	Unit	
`Configuration Items Recorded`	Jumlah item konfigurasi yang direkam untuk setiap jenis sumber daya atau semua jenis sumber daya. Item konfigurasi mewakili point-in-time tampilan berbagai atribut AWS sumber daya yang didukung. Untuk informasi selengkapnya tentang item konfigurasi atau tipe sumber daya yang didukung, lihat Item Konfigurasi dan Jenis Sumber Daya yang Didukung.	Hitungan	

Anda dapat memilih jenis sumber daya yang ingin Anda lihat dengan menggunakan daftar dropdown. Secara default, ini diatur untuk melihat semua jenis sumber daya.

AWS Config Metrik Sukses

Metrik	Deskripsi	Unit	
`Change Notifications Delivery Failed`	Jumlah pengiriman pemberitahuan perubahan yang gagal ke topik Amazon SNS untuk saluran pengiriman Anda. Pemberitahuan perubahan memberi tahu Anda tentang perubahan status konfigurasi AWS sumber daya Anda. Anda dapat menggunakan ConfigStreamDeliveryInfoAPI untuk mendapatkan `lastErrorCode` atau `lastErrorMessage` untuk pengiriman percobaan terakhir untuk pemberitahuan perubahan. Untuk informasi selengkapnya, lihat Mengelola Saluran Pengiriman.	Hitungan	

Metrik	Deskripsi	Unit	
`Config History Export Failed`	Jumlah ekspor riwayat konfigurasi yang gagal ke bucket Amazon S3 Anda. Riwayat konfigurasi adalah kumpulan item konfigura si untuk sumber daya tertentu selama periode waktu tertentu. Untuk informasi selengkap nya tentang riwayat konfigurasi, lihat Riwayat Konfigurasi.	Hitungan	
`Configura tion Recorder Insuffici ent Permissio ns Failure`	Jumlah upaya akses izin yang gagal karena kebijakan peran IAM untuk semua perekam konfigurasi di akun Anda dan Wilayah AWS memiliki izin yang tidak memadai. Perekam konfigurasi mendeteksi perubahan pada jenis sumber daya dalam lingkup. Untuk perekam konfigurasi untuk merekam konfigurasi AWS sumber daya Anda, ini memerlukan izin IAM yang diperlukan. Untuk informasi selengkapnya, lihat Kebijakan Peran IAM untuk Mendapatkan Detail Konfigurasi.	Hitungan	
`Config Snapshot Export Failed`	Jumlah snapshot konfigurasi yang gagal diekspor ke bucket Amazon S3 Anda. Snapshot konfigurasi adalah kumpulan item konfigurasi untuk sumber daya yang didukung di akun Anda. Untuk informasi selengkapnya tentang snapshot konfigurasi, lihat Snapshot Konfigurasi.	Hitungan	

Mengelola dan Melihat Konfigurasi AWS Sumber Daya dengan AWS Config

AWS Config memungkinkan Anda untuk menilai, mengaudit, dan mengevaluasi konfigurasi AWS sumber daya.

AWS sumber daya adalah entitas yang Anda buat dan kelola menggunakan AWS Management Console, AWS Command Line Interface (CLI), alat AWS SDKs, atau AWS mitra. Contoh sumber AWS daya termasuk EC2 instans Amazon, grup keamanan, Amazon VPCs, dan Amazon Elastic Block Store. AWS Config mengacu pada setiap sumber daya menggunakan pengenal uniknya, seperti ID sumber daya atau Nama Sumber Daya Amazon (ARN).

Beberapa kasus penggunaan umum meliputi:

- Administrator cloud: Anda dapat melacak dan mengelola konfigurasi sumber daya untuk membantu memastikan kepatuhan, memecahkan masalah, dan mempertahankan pemahaman tentang lingkungan Anda AWS
- Analis keamanan: Anda dapat mengevaluasi konfigurasi sumber daya terhadap status yang diinginkan untuk membantu mengidentifikasi kerentanan dan menilai postur keamanan.
- Petugas kepatuhan: Anda dapat terus mengaudit dan memantau konfigurasi sumber daya untuk membantu memastikan kepatuhan terhadap kebijakan organisasi dan standar industri.

Topik

- Jenis Sumber Daya yang Didukung untuk AWS Config
- Cakupan Sumber Daya berdasarkan Ketersediaan Wilayah
- Merekam AWS Sumber Daya dengan AWS Config
- Merekam Konfigurasi dengan AWS Config Sumber Daya Pihak Ketiga menggunakan AWS CLI
- Merekam Konfigurasi Perangkat Lunak untuk Instans Terkelola dengan AWS Config
- Mencari Sumber Daya yang Ditemukan oleh AWS Config
- Melihat Informasi Kepatuhan dan Hasil Evaluasi untuk AWS Sumber Daya Anda dengan AWS Config
- Melihat Riwayat Kepatuhan untuk AWS Sumber Daya Anda dengan AWS Config
- Menanyakan Riwayat Kepatuhan untuk Sumber Daya Anda AWS
- Menandai Sumber Daya Anda AWS Config

Jenis Sumber Daya yang Didukung untuk AWS Config

> **Important**
>
> Halaman ini diperbarui pada irama bulanan di awal setiap bulan.

AWS Config mendukung jenis AWS sumber daya dan hubungan sumber daya berikut.

- Untuk informasi lebih rinci tentang jenis sumber daya, lihat informasi referensinya (seperti sintaks, properti, dan nilai pengembalian) di referensi jenis AWS sumber daya dan properti di Panduan AWS CloudFormation Pengguna.
- Untuk AWS Config merekam, beberapa AWS Wilayah mendukung subset dari jenis sumber daya ini. Untuk informasi tentang jenis sumber daya yang didukung di Wilayah mana, lihat Cakupan Sumber Daya menurut Ketersediaan Wilayah.
- Kueri lanjutan untuk AWS Config mendukung subset dari jenis sumber daya ini. Untuk daftar jenis sumber daya yang didukung tersebut, lihat Jenis Sumber Daya yang Didukung untuk Kueri Lanjutan.
- Evaluasi proaktif untuk AWS Config mendukung subset dari jenis sumber daya ini. Untuk daftar jenis sumber daya yang didukung tersebut, lihat Jenis Sumber Daya yang Didukung untuk Evaluasi Proaktif.
- Aturan periodik berjalan tanpa perekam konfigurasi diaktifkan karena aturan periodik tidak bergantung pada item konfigurasi (CIs). Untuk informasi selengkapnya tentang perbedaan antara aturan yang dipicu perubahan dan aturan periodik, lihat Mode Evaluasi dan Jenis Pemicu untuk Aturan. AWS Config

  Ini berarti bahwa jika Anda melihat halaman aturan, tidak ada CI terdaftar atau sumber daya yang didukung. Jika Anda memilih ID sumber daya, Anda akan melihat kesalahan berikut:The `provided resource ID and resource type cannot be found`. Ini adalah perilaku yang diharapkan.

> **Note**
>
> Ketersediaan wilayah untuk jenis sumber daya
> Sebelum menentukan jenis sumber daya AWS Config untuk dilacak, periksa Cakupan Sumber Daya menurut Ketersediaan Wilayah untuk melihat apakah jenis sumber daya

didukung di AWS Wilayah tempat Anda menyiapkan AWS Config. Jika jenis sumber daya didukung oleh AWS Config setidaknya satu Wilayah, Anda dapat mengaktifkan perekaman jenis sumber daya tersebut di semua Wilayah yang didukung oleh AWS Config, meskipun jenis sumber daya yang ditentukan tidak didukung di AWS Wilayah tempat Anda menyiapkan AWS Config.

Menandai dukungan untuk jenis sumber daya

Jika tipe sumber daya tidak mendukung penandaan atau tidak menyertakan informasi tag dalam respons API deskripsinya, tidak AWS Config akan menangkap data tag dalam item konfigurasi (CIs) untuk jenis sumber daya tersebut. AWS Config masih akan mencatat sumber daya ini. Namun, fungsionalitas apa pun yang bergantung pada data tag tidak akan berfungsi. Ini memengaruhi pemfilteran, pengelompokan, atau evaluasi kepatuhan berbasis tag yang bergantung pada data tag.

Amazon AppStream

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon AppStream	`AWS::AppStream::DirectoryConfig`	TA	TA
	`AWS::AppStream::Application`	TA	TA
	`AWS::AppStream::Stack`	TA	TA
	`AWS::AppStream::Fleet`	TA	TA

Amazon AppFlow

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon AppFlow	`AWS::AppFlow::Flow`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon AppIntegrations	`AWS::AppIntegrations::EventIntegration`	TA	TA
	`AWS::AppIntegrations::Application`	TA	TA

Amazon API Gateway

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
API Gateway	`AWS::ApiGateway::Stage`	terkandung dalam	ApiGateway Istirahat Api
		dikaitkan dengan	WAFRegional WebACL

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::ApiGateway::RestApi`	mengandung	ApiGateway Panggung
API Gateway V2	`AWS::ApiGatewayV2::Stage`	terkandung dalam	ApiGatewayV2 Api
	`AWS::ApiGatewayV2::Api`	mengandung	ApiGatewayTahap V2

Untuk mempelajari selengkapnya tentang cara AWS Config mengintegrasikan dengan Amazon API Gateway, lihat Memantau Konfigurasi API Gateway API dengan AWS Config.

Amazon Athena

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Athena	`AWS::Athena::WorkGroup`	TA	TA
	`AWS::Athena::DataCatalog`	TA	TA
	`AWS::Athena::PreparedStatement`	TA	TA

Amazon Bedrock

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Bedrock	`AWS::Bedrock::Guardrail`	TA	TA
	`AWS::Bedrock::KnowledgeBase`	TA	TA

Amazon CloudFront

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon CloudFront	`AWS::CloudFront::Distribution`	dikaitkan dengan	AWS WAF WebACL
			Sertifikat ACM
			Bucket S3
			Sertifikat Server IAM
	`AWS::CloudFront::PublicKey`	TA	TA
	`AWS::CloudFront::StreamingDistribution`	dikaitkan dengan	AWS WAF WebACL
			Sertifikat ACM
			Bucket S3
			Sertifikat Server IAM

Amazon CloudWatch

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon CloudWatch	`AWS::CloudWatch::Alarm`	TA	TA
	`AWS::CloudWatch::MetricStream`	TA	TA
CloudWatch Log Amazon	`AWS::Logs::Destination`	TA	TA
Amazon CloudWatch RUM	`AWS::RUM::AppMonitor`	TA	TA
Amazon CloudWatch Terbukti	`AWS::Evidently::Project`	TA	TA
	`AWS::Evidently::Launch`	TA	TA
	`AWS::Evidently::Segment`	TA	TA

Amazon CodeGuru

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
CodeGuru Peninjau Amazon	`AWS::CodeGuruReviewer::RepositoryAssociation`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon CodeGuru Profiler	`AWS::CodeGuruProfiler::ProfilingGroup`	TA	TA

Amazon Cognito

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Cognito	`AWS::Cognito::UserPool`	TA	TA
	`AWS::Cognito::UserPoolClient`	TA	TA
	`AWS::Cognito::UserPoolGroup`	TA	TA
	`AWS::Cognito::IdentityPool`	TA	TA

Amazon Connect

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Connect	`AWS::Connect::PhoneNumber`	TA	TA
	`AWS::Connect::QuickConnect`	TA	TA
	`AWS::Connect::Instance`	TA	TA
	`AWS::Connect::Rule`	TA	TA
	`AWS::Connect::User`	TA	TA
Amazon Connect Customer Profiles	`AWS::CustomerProfiles::Domain`	TA	TA
	`AWS::CustomerProfiles::ObjectType`	TA	TA

Amazon Detective

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Detective	`AWS::Detective::Graph`	TA	TA

Amazon DynamoDB

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon DynamoDB	`AWS::DynamoDB::Table`	TA	TA

Amazon Elastic Compute Cloud

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Elastic Compute Cloud	`AWS::EC2::Host` *	mengandung	EC2 contoh
	`AWS::EC2::EIP`	melekat pada	EC2 contoh
			Antarmuka jaringan
	`AWS::EC2::Instance`	mengandung	EC2 antarmuka jaringan
		dikaitkan dengan	EC2 kelompok keamanan
		melekat pada	Volume Amazon EBS
			EC2 IP elastis (EIP)

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
		terkandung dalam	EC2 Tuan rumah khusus
			Tabel rute
			Subnet
			Cloud privat virtual (VPC)
	`AWS::EC2::NetworkInterface`	dikaitkan dengan	EC2 kelompok keamanan
		melekat pada	EC2 IP elastis (EIP)
			EC2 contoh
		terkandung dalam	Tabel rute
			Subnet
			Cloud privat virtual (VPC)
	`AWS::EC2::SecurityGroup` *	dikaitkan dengan	EC2 contoh
			EC2 antarmuka jaringan
			Cloud privat virtual (VPC)
	`AWS::EC2::NatGateway`	terkandung dalam	Cloud privat virtual (VPC)
		terkandung dalam	Subnet

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::EC2::EgressOnlyInternetGateway`	melekat pada	Cloud privat virtual (VPC)
	`AWS::EC2::EC2Fleet`	TA	TA
	`AWS::EC2::SpotFleet`	TA	TA
	`AWS::EC2::PrefixList`	TA	TA
	`AWS::EC2::FlowLog`	TA	TA
	`AWS::EC2::TransitGateway`	TA	TA
	`AWS::EC2::TransitGatewayAttachment`	TA	TA
	`AWS::EC2::TransitGatewayRouteTable`	TA	TA
	`AWS::EC2::VPCEndpoint`	terkandung dalam	Cloud privat virtual (VPC)
		melekat pada	Antarmuka jaringan

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
		terkandung dalam	Subnet
		terkandung dalam	Tabel rute
	`AWS::EC2::VPCEndpointService`	dikaitkan dengan	ElasticLoadBalancingV2 LoadBalancer
	`AWS::EC2::VPCPeeringConnection`	dikaitkan dengan	Cloud privat virtual (VPC)
	`AWS::EC2::RegisteredHAInstance`	dikaitkan dengan	EC2 contoh
	`AWS::EC2::SubnetRouteTableAssociation`	TA	TA
	`AWS::EC2::LaunchTemplate`	TA	TA
	`AWS::EC2::NetworkInsightsAccessScopeAnalysis`	TA	TA
	`AWS::EC2::TrafficMirrorTarget`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::EC2::TrafficMirrorSession`	TA	TA
	`AWS::EC2::DHCPOptions`	TA	TA
	`AWS::EC2::IPAM`	TA	TA
	`AWS::EC2::IPAMResourceDiscovery`	TA	TA
	`AWS::EC2::IPAMResourceDiscoveryAssociation`	TA	TA
	`AWS::EC2::NetworkInsightsPath`	TA	TA
	`AWS::EC2::TrafficMirrorFilter`	TA	TA
	`AWS::EC2::CapacityReservation`	TA	TA
	`AWS::EC2::ClientVpnEndpoint`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::EC2::Customer Gateway`	melekat pada	Koneksi VPN
	`AWS::EC2::Internet Gateway`	melekat pada	Cloud privat virtual (VPC)
	`AWS::EC2::NetworkAcl`	TA	TA
	`AWS::EC2::RouteTable`	mengandung	EC2 contoh
			EC2 antarmuka jaringan
			Subnet
			Gateway VPN
		terkandung dalam	Cloud privat virtual (VPC)
	`AWS::EC2::Subnet`	mengandung	EC2 contoh
			EC2 antarmuka jaringan
		melekat pada	ACL jaringan
		terkandung dalam	Tabel rute
			Cloud privat virtual (VPC)
	`AWS::EC2::VPC`	mengandung	EC2 contoh

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
			EC2 antarmuka jaringan
			ACL jaringan
			Tabel rute
			Subnet
		dikaitkan dengan	Grup keamanan
		melekat pada	gateway internet
			Gateway VPN
	`AWS::EC2::VPNConnection`	melekat pada	Gateway pelanggan
			Gateway VPN
	`AWS::EC2::VPNConnectionRoute`	TA	TA
	`AWS::EC2::VPNGateway`	melekat pada	Cloud privat virtual (VPC)
			Koneksi VPN
		terkandung dalam	Tabel rute
	`AWS::EC2::IPAMScope`	TA	TA
	`AWS::EC2::CarrierGateway`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::EC2::TransitGatewayConnect`	TA	TA
	`AWS::EC2::IPAMPool`	TA	TA
	`AWS::EC2::TransitGatewayMulticastDomain`	TA	TA
	`AWS::EC2::NetworkInsightsAccessScope`	TA	TA
	`AWS::EC2::NetworkInsightsAnalysis`	TA	TA
	`AWS::EC2::VPCBlockPublicAccessOptions`	TA	TA
	`AWS::EC2::VPCBlockPublicAccessExclusion`	TA	TA
	`AWS::EC2::EIPAssociation`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::EC2::InstanceConnectEndpoint`	TA	TA
	`AWS::EC2::SnapshotBlockPublicAccess`	TA	TA
	`AWS::EC2::VPCEndpointConnectionNotification`	TA	TA
Amazon Elastic Block Store	`AWS::EC2::Volume`	melekat pada	EC2 contoh
EC2 Image Builder	`AWS::ImageBuilder::ImagePipeline`	TA	TA
	`AWS::ImageBuilder::DistributionConfiguration`	TA	TA
	`AWS::ImageBuilder::ContainerRecipe`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::ImageBuilder::InfrastructureConfiguration`	TA	TA
	`AWS::ImageBuilder::ImageRecipe`	TA	TA

*AWS Config mencatat detail konfigurasi Host khusus dan instance yang Anda luncurkan pada host tersebut. Akibatnya, Anda dapat menggunakannya AWS Config sebagai sumber data saat melaporkan kepatuhan terhadap lisensi perangkat lunak terikat server Anda. Misalnya, Anda dapat melihat riwayat konfigurasi instance dan menentukan Amazon Machine Image (AMI) yang menjadi dasarnya. Kemudian, Anda dapat mencari riwayat konfigurasi host, yang mencakup detail seperti jumlah soket dan inti, untuk memeriksa apakah host mematuhi persyaratan lisensi AMI. Untuk informasi selengkapnya, lihat Melacak Perubahan Konfigurasi dengan AWS Config di Panduan EC2 Pengguna Amazon.

* Definisi EC2 SecurityGroup Properti berisi blok IP CIDR, yang dikonversi ke rentang IP secara internal, dan dapat mengembalikan hasil yang tidak terduga ketika mencoba menemukan rentang IP tertentu. Untuk solusi untuk mencari rentang IP tertentu, lihat Batasan untuk Kueri Lanjutan.

Amazon Elastic Container Registry

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Elastic Container Registry	`AWS::ECR::Repository`	TA	TA
	`AWS::ECR::RegistryPolicy`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::ECR::PullThroughCacheRule`	TA	TA
Amazon Elastic Container Registry Publik	`AWS::ECR::PublicRepository`	TA	TA

Amazon Elastic Container Service

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Elastic Container Service	`AWS::ECS::Cluster`	TA	TA
	`AWS::ECS::TaskDefinition`	TA	TA
	`AWS::ECS::Service` *	TA	TA
	`AWS::ECS::TaskSet`	TA	TA
	`AWS::ECS::CapacityProvider`	TA	TA

* Layanan ini saat ini hanya mendukung format Amazon Resource Name (ARN) yang baru. Untuk informasi selengkapnya, lihat Amazon Resource Names (ARNs) dan IDs di panduan pengembang ECS.

Lama (tidak didukung): `arn:aws:ecs:region:aws_account_id:service/service-name`

Baru (didukung): `arn:aws:ecs:region:aws_account_id:service/cluster-name/service-name`

Sistem File Elastis Amazon

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Sistem File Elastis Amazon	`AWS::EFS::FileSystem`	TA	TA
	`AWS::EFS::AccessPoint`	TA	TA

Amazon Elastic Kubernetes Service

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Elastic Kubernetes Service	`AWS::EKS::Cluster`	TA	TA
	`AWS::EKS::FargateProfile`	TA	TA
	`AWS::EKS::IdentityProviderConfig`	TA	TA
	`AWS::EKS::Addon`	TA	TA

Amazon EMR

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon EMR	`AWS::EMR::Security Configuration`	TA	TA

Amazon EventBridge

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon EventBridge	`AWS::Events::EventBus`	TA	TA
	`AWS::Events::ApiDestination`	TA	TA
	`AWS::Events::Archive`	TA	TA
	`AWS::Events::Endpoint`	TA	TA
	`AWS::Events::Connection`	TA	TA
	`AWS::Events::Rule`	TA	TA
EventBridge Skema Amazon	`AWS::EventSchemas::Registry Policy`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::EventSchemas::Discoverer`	TA	TA
	`AWS::EventSchemas::Schema`	TA	TA
	`AWS::EventSchemas::Registry`	TA	TA

Amazon Forecast

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Forecast	`AWS::Forecast::Dataset`	TA	TA
	`AWS::Forecast::DatasetGroup`	TA	TA

Amazon Fraud Detector

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Fraud Detector	`AWS::FraudDetector::Label`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::FraudDetector::EntityType`	TA	TA
	`AWS::FraudDetector::Variable`	TA	TA
	`AWS::FraudDetector::Outcome`	TA	TA

Amazon GuardDuty

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon GuardDuty	`AWS::GuardDuty::Detector`	TA	TA
	`AWS::GuardDuty::ThreatIntelSet`	TA	TA
	`AWS::GuardDuty::IPSet`	TA	TA
	`AWS::GuardDuty::Filter`	TA	TA

Amazon Inspector

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Inspector	`AWS::InspectorV2::Filter`	TA	TA
	`AWS::InspectorV2::Activation`	TA	TA

Amazon Interactive Video Service

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Interactive Video Service	`AWS::IVS::Channel`	TA	TA
	`AWS::IVS::RecordingConfiguration`	TA	TA
	`AWS::IVS::PlaybackKeyPair`	TA	TA

Amazon Keyspaces (untuk Apache Cassandra)

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Keyspaces (untuk Apache Cassandra)	`AWS::Cassandra::Keyspace`	TA	TA

OpenSearch Layanan Amazon

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
OpenSearch Layanan Amazon (Elasticsearch lama)	`AWS::Elasticsearch::Domain`	dikaitkan dengan	Kunci KMS
			EC2 kelompok keamanan
			EC2 subnet
			Cloud privat virtual (VPC)
OpenSearch Layanan Amazon	`AWS::OpenSearch::Domain`	TA	TA
Amazon Tanpa OpenSearch Server	`AWS::OpenSearchServerless::VpcEndpoint`	TA	TA
	`AWS::OpenSearchServerless::Collection`	TA	TA

> **Ganti nama OpenSearch Layanan Amazon**
>
> Pada 8 September 2021, Amazon Elasticsearch Service diubah namanya menjadi Amazon Service. OpenSearch OpenSearch Layanan mendukung OpenSearch serta warisan Elasticsearch OSS. Untuk informasi selengkapnya, lihat OpenSearch Layanan Amazon - Ringkasan perubahan.
>
> Anda dapat terus melihat data Anda `AWS::OpenSearch::Domain` di bawah jenis `AWS::Elasticsearch::Domain` sumber daya yang ada selama beberapa minggu, bahkan jika Anda memutakhirkan satu atau beberapa domain ke OpenSearch.

Amazon Personalize

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Personalize	`AWS::Personalize::Dataset`	TA	TA
	`AWS::Personalize::Schema`	TA	TA
	`AWS::Personalize::Solution`	TA	TA
	`AWS::Personalize::DatasetGroup`	TA	TA

Amazon Pinpoint

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Pinpoint	`AWS::Pinpoint::ApplicationSettings`	TA	TA
	`AWS::Pinpoint::Segment`	TA	TA
	`AWS::Pinpoint::App`	TA	TA
	`AWS::Pinpoint::Campaign`	TA	TA
	`AWS::Pinpoint::InAppTemplate`	TA	TA
	`AWS::Pinpoint::EmailChannel`	TA	TA
	`AWS::Pinpoint::EmailTemplate`	TA	TA
	`AWS::Pinpoint::EventStream`	TA	TA

Amazon Quantum Ledger Database (Amazon QLDB)

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon QLDB	`AWS::QLDB::Ledger`	TA	TA

Amazon Kendra

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Kendra	`AWS::Kendra::Index`	TA	TA

Amazon Kinesis

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Kinesis	`AWS::Kinesis::Stream`	TA	TA
	`AWS::Kinesis::StreamConsumer`	TA	TA
Amazon Kinesis Analytics V2	`AWS::KinesisAnalyticsV2::Application`	TA	TA
Amazon Data Firehose	`AWS::KinesisFireho`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`se::DeliveryStream`		
Aliran video Kinesis	`AWS::KinesisVideo::SignalingChannel`	TA	TA
	`AWS::KinesisVideo::Stream`	TA	TA

Amazon Lex

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Lex	`AWS::Lex::BotAlias`	TA	TA
	`AWS::Lex::Bot`	TA	TA

Amazon Lightsail

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Lightsail	`AWS::Lightsail::Disk`	TA	TA
	`AWS::Lightsail::Certificate`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::Lightsail::Bucket`	TA	TA
	`AWS::Lightsail::StaticIp`	TA	TA

Amazon Lookout for Metrics

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Lookout for Metrics	`AWS::LookoutMetrics::Alert`	TA	TA

Amazon Lookout for Vision

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Lookout for Vision	`AWS::LookoutVision::Project`	TA	TA

Amazon Macie

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Macie	`AWS::Macie::Session`	TA	TA

Amazon Managed Grafana

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Managed Grafana	`AWS::Grafana::Workspace`	TA	TA

Layanan Terkelola Amazon untuk Prometheus

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Layanan Terkelola Amazon untuk Prometheus	`AWS::APS::RuleGroupsNamespace`	TA	TA

Amazon MemoryDB

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon MemoryDB	`AWS::MemoryDB::SubnetGroup`	TA	TA

Amazon MQ

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon MQ	`AWS::AmazonMQ::Broker`	TA	TA

Amazon Managed Streaming untuk Apache Kafka

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Managed Streaming untuk Apache Kafka	`AWS::MSK::Cluster`	TA	TA
	`AWS::MSK::Configuration`	TA	TA
	`AWS::MSK::BatchScramSecret`	TA	TA
	`AWS::MSK::ClusterPolicy`	TA	TA
	`AWS::MSK::VpcConnection`	TA	TA
Amazon Managed Streaming for Apache Kafka Connect	`AWS::KafkaConnect::Connector`	TA	TA

Amazon QuickSight

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon QuickSight	`AWS::QuickSight::DataSource`	TA	TA
	`AWS::QuickSight::Template`	TA	TA
	`AWS::QuickSight::Theme`	TA	TA

Amazon Redshift

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Redshift	`AWS::Redshift::Cluster`	dikaitkan dengan	Grup parameter klaster
			Grup keamanan klaster
			Kelompok subnet cluster
			Grup keamanan
			Cloud privat virtual (VPC)
	`AWS::Redshift::Clu`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`sterParameterGroup`		
	`AWS::Redshift::ClusterSecurityGroup`	TA	TA
	`AWS::Redshift::ScheduledAction`	TA	TA
	`AWS::Redshift::ClusterSnapshot`	dikaitkan dengan	Klaster
			Cloud privat virtual (VPC)
	`AWS::Redshift::ClusterSubnetGroup`	dikaitkan dengan	Subnet
			Cloud privat virtual (VPC)
	`AWS::Redshift::EventSubscription`	TA	TA
	`AWS::Redshift::EndpointAccess`	TA	TA
	`AWS::Redshift::EndpointAuthorization`	TA	TA

Amazon Relational Database Service

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Relational Database Service	`AWS::RDS::DBCluster`	mengandung	Contoh RDS DB
		dikaitkan dengan	Grup subnet RDS DB
			EC2 kelompok keamanan
	`AWS::RDS::DBClusterSnapshot`	dikaitkan dengan	Kluster RDS DB
			Cloud privat virtual (VPC)
	`AWS::RDS::DBInstance`	dikaitkan dengan	EC2 kelompok keamanan
			Grup keamanan RDS DB
			Grup subnet RDS DB
	`AWS::RDS::DBSecurityGroup`	dikaitkan dengan	EC2 kelompok keamanan
			Cloud privat virtual (VPC)
	`AWS::RDS::DBSnapshot`	dikaitkan dengan	Cloud privat virtual (VPC)
	`AWS::RDS::DBSubnetGroup`	dikaitkan dengan	EC2 kelompok keamanan
			Cloud privat virtual (VPC)

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::RDS::EventSubscription`	TA	TA
	`AWS::RDS::GlobalCluster`	TA	TA
	`AWS::RDS::Integration`	TA	TA
	`AWS::RDS::OptionGroup`	TA	TA

Amazon Route 53

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Route 53	`AWS::Route53::HostedZone`	TA	TA
	`AWS::Route53::HealthCheck`	TA	TA
Profil Amazon Route 53	`AWS::Route53Profiles::Profile`	TA	TA
Amazon Route 53 Resolver	`AWS::Route53Resolver::ResolverEndpoint`	TA	TA
	`AWS::Route53Resolver::ResolverRule`	TA	TA
	`AWS::Route53Resolver::ResolverRuleAssociation`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	AWS::Route53Resolver::FirewallDomainList	TA	TA
	AWS::Route53Resolver::FirewallRuleGroupAssociation	TA	TA
	AWS::Route53Resolver::ResolverQueryLoggingConfig	TA	TA
	AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	TA	TA
	AWS::Route53Resolver::FirewallRuleGroup	TA	TA
Pengontrol Pemulihan Aplikasi Amazon (ARC)	AWS::Route53RecoveryReadiness::Cell	TA	TA
	AWS::Route53RecoveryReadiness::ReadinessCheck	TA	TA
	AWS::Route53RecoveryReadiness::RecoveryGroup	TA	TA
	AWS::Route53RecoveryControl::Cluster	TA	TA
	AWS::Route53RecoveryControl::ControlPanel	TA	TA
	AWS::Route53RecoveryControl::RoutingControl	TA	TA
	AWS::Route53RecoveryControl::SafetyRule	TA	TA
	AWS::Route53RecoveryReadiness::ResourceSet	TA	TA

Amazon SageMaker AI

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon SageMaker AI	`AWS::SageMaker::CodeRepository`	TA	TA
	`AWS::SageMaker::Domain`	TA	TA
	`AWS::SageMaker::AppImageConfig`	TA	TA
	`AWS::SageMaker::Image`	TA	TA
	`AWS::SageMaker::Model`	TA	TA
	`AWS::SageMaker::NotebookInstance`	TA	TA
	`AWS::SageMaker::NotebookInstanceLifecycleConfig`	TA	TA
	`AWS::SageMaker::EndpointConfig`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::SageMaker::Workteam`	TA	TA
	`AWS::SageMaker::FeatureGroup`	TA	TA
	`AWS::SageMaker::InferenceExperiment`	TA	TA

Layanan Email Sederhana Amazon

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Layanan Email Sederhana Amazon	`AWS::SES::ConfigurationSet`	TA	TA
	`AWS::SES::ContactList`	TA	TA
	`AWS::SES::Template`	TA	TA
	`AWS::SES::ReceiptFilter`	TA	TA
	`AWS::SES::ReceiptRuleSet`	TA	TA

Amazon Simple Notification Service

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Simple Notification Service	`AWS::SNS::Topic`	TA	TA

Amazon Simple Queue Service

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Simple Queue Service	`AWS::SQS::Queue`	TA	TA

Amazon Simple Storage Service

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon Simple Storage Service	`AWS::S3::Bucket` *	TA	TA
	`AWS::S3::AccountPublicAccessBlock`	TA	TA
	`AWS::S3::MultiRegionAccessPoint`	TA	TA
	`AWS::S3::StorageLens`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::S3::AccessPoint`	TA	TA
	`AWS::S3::StorageLensGroup`	TA	TA
	`AWS::S3Tables::TableBucket`	TA	TA
Amazon S3 Express Satu Zona	`AWS::S3Express::DirectoryBucket`	TA	TA
	`AWS::S3Express::BucketPolicy`	TA	TA

* Jika Anda mengonfigurasi AWS Config untuk merekam bucket S3, dan tidak menerima pemberitahuan perubahan konfigurasi, periksa apakah kebijakan bucket S3 Anda memiliki izin yang diperlukan. Untuk informasi selengkapnya, lihat Mengelola Izin untuk Perekaman Bucket S3.

Atribut Bucket Amazon S3

AWS Config juga mencatat atribut berikut untuk jenis sumber daya bucket Amazon S3.

Atribut	Deskripsi
AccelerateConfiguration	Transfer akselerasi untuk data jarak jauh antara klien Anda dan ember.
BucketAcl	Daftar kontrol akses digunakan untuk mengelola akses ke bucket dan objek.

Atribut	Deskripsi
BucketPolicy	Kebijakan yang menentukan izin ke bucket.
CrossOriginConfiguration	Izinkan permintaan lintas asal ke bucket.
LifecycleConfiguration	Aturan yang menentukan siklus hidup objek di bucket Anda.
LoggingConfiguration	Logging digunakan untuk melacak permintaan akses ke bucket.
NotificationConfiguration	Pemberitahuan peristiwa yang digunakan untuk mengirim peringatan atau memicu alur kerja untuk peristiwa bucket tertentu.
ReplicationConfiguration	Penyalinan objek secara otomatis dan asinkron di seluruh ember di Wilayah yang berbeda. AWS
RequestPaymentConfiguration	Pemohon membayar diaktifkan.
TaggingConfiguration	Tag ditambahkan ke ember untuk dikategorikan. Anda juga dapat menggunakan penandaan untuk melacak penagihan.
WebsiteConfiguration	Hosting situs web statis diaktifkan untuk ember.
VersioningConfiguration	Pembuatan versi diaktifkan untuk objek di ember.

Untuk informasi selengkapnya tentang atribut, lihat Opsi Konfigurasi Bucket di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Amazon WorkSpaces

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Amazon WorkSpaces	`AWS::WorkSpaces::ConnectionAlias`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::WorkSpaces::Workspace`	TA	TA

AWS Amplify

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Amplify	`AWS::Amplify::App`	TA	TA
	`AWS::Amplify::Branch`	TA	TA

AWS AppConfig

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS AppConfig	`AWS::AppConfig::Application`	TA	TA
	`AWS::AppConfig::Environment`	TA	TA
	`AWS::AppConfig::ConfigurationProfile`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::AppConfig::DeploymentStrategy`	TA	TA
	`AWS::AppConfig::HostedConfigurationVersion`	TA	TA
	`AWS::AppConfig::ExtensionAssociation`	TA	TA

AWS App Runner

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS App Runner	`AWS::AppRunner::VpcConnector`	TA	TA
	`AWS::AppRunner::Service`	TA	TA

AWS App Mesh

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS App Mesh	`AWS::AppMesh::VirtualNode`	TA	TA
	`AWS::AppMesh::VirtualService`	TA	TA
	`AWS::AppMesh::VirtualGateway`	TA	TA
	`AWS::AppMesh::VirtualRouter`	TA	TA
	`AWS::AppMesh::Route`	TA	TA
	`AWS::AppMesh::GatewayRoute`	TA	TA
	`AWS::AppMesh::Mesh`	TA	TA

AWS AppSync

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS AppSync	`AWS::AppSync::GraphQLApi`	TA	TA

AWS Audit Manager

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Audit Manager	`AWS::AuditManager::Assessment`	TA	TA

AWS Auto Scaling

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`	mengandung	EC2 Contoh Amazon
		dikaitkan dengan	Classic Load Balancer
			Konfigurasi peluncuran Auto Scaling
			Subnet
	`AWS::AutoScaling::`	dikaitkan dengan	Grup EC2 keamanan Amazon

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`LaunchConfiguration`		
	`AWS::AutoScaling::ScalingPolicy`	dikaitkan dengan	Grup Auto Scaling
			Alarm
	`AWS::AutoScaling::ScheduledAction`	dikaitkan dengan	Grup Auto Scaling
	`AWS::AutoScaling::WarmPool`	TA	TA

AWS Backup

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Backup	`AWS::Backup::BackupPlan`	TA	NA *
	`AWS::Backup::BackupSelection`	TA	TA
	`AWS::Backup::BackupVault`	TA	NA *

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::Backup::RecoveryPoint`	TA	TA
	`AWS::Backup::ReportPlan`	TA	TA
AWS Gerbang Cadangan	`AWS::BackupGateway::Hypervisor`	TA	TA

Karena cara AWS Backup kerjanya, beberapa jenis sumber daya ini berhubungan dengan jenis AWS Backup sumber daya lain dalam tabel ini.

`AWS::Backup::BackupPlan`terkait dengan `AWS::Backup::BackupSelection` di mana Rencana Cadangan memiliki banyak pilihan, dan `AWS::Backup::BackupVault` terkait dengan `AWS::Backup::RecoveryPoint` tempat AWS Backup Vault memiliki beberapa titik pemulihan.

Untuk informasi selengkapnya, lihat Mengelola cadangan menggunakan paket cadangan dan Bekerja dengan brankas cadangan.

AWS Batch

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Batch	`AWS::Batch::JobQueue`	TA	TA
	`AWS::Batch::ComputeEnvironment`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::Batch::SchedulingPolicy`	TA	TA

AWS Manajemen Penagihan dan Biaya

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Manajemen Penagihan dan Biaya	`AWS::BCMDataExports::Export`	TA	TA

AWS Budgets

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Budgets	`AWS::Budgets::BudgetsAction`	TA	TA

AWS Certificate Manager

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Certificate Manager	`AWS::ACM::Certificate`	TA	TA

AWS CloudFormation

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS CloudFormation	`AWS::CloudFormation::GuardHook`	TA	TA
	`AWS::CloudFormation::Stack` *	mengandung	Jenis AWS sumber daya yang didukung

*AWS Config mencatat perubahan konfigurasi ke AWS CloudFormation tumpukan dan jenis sumber daya yang didukung di tumpukan. AWS Config tidak merekam perubahan konfigurasi untuk jenis sumber daya di tumpukan yang belum didukung. Jenis sumber daya yang tidak didukung muncul di bagian konfigurasi tambahan dari item konfigurasi untuk tumpukan.

AWS CloudTrail

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS CloudTrail	`AWS::CloudTrail::Trail`	TA	TA

AWS Cloud9

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Cloud9	`AWS::Cloud9::EnvironmentEC2`	TA	TA

> **AWS Cloud9 akses tidak lagi tersedia untuk pengguna baru**
>
> Setelah mempertimbangkan dengan cermat, kami telah membuat keputusan untuk menutup akses pelanggan baru AWS Cloud9, efektif 25 Juli 2024. AWS Cloud9 Pelanggan yang sudah ada dapat terus menggunakan layanan seperti biasa. AWS terus berinvestasi dalam keamanan, ketersediaan, dan peningkatan kinerja untuk AWS Cloud9, tetapi kami tidak berencana untuk memperkenalkan fitur baru. Untuk informasi selengkapnya, lihat Cara bermigrasi dari AWS Cloud9 ke Toolkit AWS IDE atau. AWS CloudShell

AWS Cloud Map

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Penemuan Layanan	`AWS::ServiceDiscovery::Service`	TA	TA
	`AWS::ServiceDiscovery::PublicDnsNamespace`	TA	TA
	`AWS::ServiceDiscovery::HttpNamespace`	TA	TA
`AWS::ServiceDiscovery::Instance`	TA	TA	

AWS CodeArtifact

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS CodeArtifact	`AWS::CodeArtifact::Repository`	TA	TA

AWS CodeBuild

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS CodeBuild	`AWS::CodeBuild::Project` *	dikaitkan dengan	Bucket S3
			Peran IAM
	`AWS::CodeBuild::ReportGroup`	TA	TA

* Untuk mempelajari lebih lanjut tentang cara AWS Config mengintegrasikan dengan AWS CodeBuild, lihat Menggunakan AWS Config dengan AWS CodeBuild Sampel.

AWS CodeDeploy

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS CodeDeploy	`AWS::CodeDeploy::Application`	mengandung	DeploymentGroup
	`AWS::CodeDeploy::D`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`eployment Config`		
	`AWS::Code Deploy::D eploymentGroup`	terkandung dalam	Aplikasi

AWS CodePipeline

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS CodePipeline	`AWS::Code Pipeline: :Pipeline` *	melekat pada	Bucket S3
		dikaitkan dengan	Peran IAM
			Proyek kode
			Fungsi Lambda
			Tumpukan cloudform ation
			ElasticBeanstalk aplikasi

*AWS Config mencatat perubahan konfigurasi ke CodePipeline saluran pipa dan jenis sumber daya yang didukung di saluran pipa. AWS Config tidak mencatat perubahan konfigurasi untuk jenis sumber daya di pipeline yang belum didukung. Jenis sumber daya yang tidak didukung seperti `CodeCommit repository`, `CodeDeploy application`, `ECS cluster`, dan `ECS service` muncul di bagian konfigurasi tambahan dari item konfigurasi untuk tumpukan.

AWS Config

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Config	`AWS::Config::ResourceCompliance` *	dikaitkan dengan	Semua sumber daya*
	`AWS::Config::ConformancePackCompliance`	TA	TA
	`AWS::Config::ConfigurationRecorder` *	TA	TA

* Hubungan antara `AWS::Config::ResourceCompliance` dan sumber daya terkait tergantung pada bagaimana `AWS::Config::ResourceCompliance` melaporkan kepatuhan untuk jenis sumber daya tertentu.

* `AWS::Config::ConfigurationRecorder` adalah jenis sumber daya sistem AWS Config dan perekaman jenis sumber daya ini diaktifkan secara default.

> **Note**
>
> Rekaman untuk jenis `AWS::Config::ConformancePackCompliance` dan `AWS::Config::ConfigurationRecorder` sumber daya datang tanpa biaya tambahan.

AWS Database Migration Service

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Database Migration Service	`AWS::DMS::EventSubscription`	TA	TA
	`AWS::DMS::ReplicationSubnetGroup`	TA	TA
	`AWS::DMS::ReplicationInstance`	TA	TA
	`AWS::DMS::ReplicationTask`	TA	TA
	`AWS::DMS::Certificate`	TA	TA
	`AWS::DMS::Endpoint`	TA	TA

AWS DataSync

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS DataSync	`AWS::DataSync::LocationSMB`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::DataSync::LocationFSxLustre`	TA	TA
	`AWS::DataSync::LocationFSxWindows`	TA	TA
	`AWS::DataSync::LocationS3`	TA	TA
	`AWS::DataSync::LocationEFS`	TA	TA
	`AWS::DataSync::LocationNFS`	TA	TA
	`AWS::DataSync::LocationHDFS`	TA	TA
	`AWS::DataSync::LocationObjectStorage`	TA	TA
	`AWS::DataSync::Task`	TA	TA

AWS Device Farm

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Device Farm	`AWS::DeviceFarm::TestGridProject`	TA	TA
	`AWS::DeviceFarm::InstanceProfile`	TA	TA
	`AWS::DeviceFarm::Project`	TA	TA

AWS Elastic Beanstalk

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Application`	mengandung	Versi Aplikasi Elastic Beanstalk
			Lingkungan Elastic Beanstalk
		dikaitkan dengan	Peran IAM
	`AWS::ElasticBeanstalk::ApplicationVersion`	terkandung dalam	Aplikasi Elastic Beanstalk
		dikaitkan dengan	Lingkungan Elastic Beanstalk
			Bucket S3

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::ElasticBeanstalk::Environment`	terkandung dalam	Aplikasi Elastic Beanstalk
		dikaitkan dengan	Versi Aplikasi Elastic Beanstalk
			Peran IAM
		mengandung	CloudFormation Tumpukan

Resolusi Entitas AWS

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Resolusi Entitas AWS	`AWS::EntityResolution::IdMappingWorkflow`	TA	TA
	`AWS::EntityResolution::SchemaMapping`	TA	TA

AWS Fault Injection Service

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Fault Injection Service	`AWS::FIS::ExperimentTemplate`	TA	TA

AWS Global Accelerator

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Global Accelerator	`AWS::GlobalAccelerator::Listener`	TA	TA
	`AWS::GlobalAccelerator::EndpointGroup`	TA	TA
	`AWS::GlobalAccelerator::Accelerator`	TA	TA

AWS Glue

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Glue	`AWS::Glue::Job`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::Glue::Classifier`	TA	TA
	`AWS::Glue::MLTransform`	TA	TA

AWS Ground Station

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Ground Station	`AWS::GroundStation::Config`	TA	TA
	`AWS::GroundStation::MissionProfile`	TA	TA
	`AWS::GroundStation::DataflowEndpointGroup`	TA	TA

AWS HealthLake

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS HealthLake	`AWS::HealthLake::FHIRDatastore`	TA	TA

AWS Identity and Access Management (IAM)

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Identity and Access Management	`AWS::IAM::User`	melekat pada	Grup IAM
			Kebijakan yang dikelola pelanggan IAM
	`AWS::IAM::Group`	mengandung	Pengguna IAM
		melekat pada	Kebijakan yang dikelola pelanggan IAM
	`AWS::IAM::Role`	melekat pada	Kebijakan yang dikelola pelanggan IAM
	`AWS::IAM::Policy`	melekat pada	Pengguna IAM
			Grup IAM
			Peran IAM

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::IAM::SAMLProvider`	TA	TA
	`AWS::IAM::ServerCertificate`	TA	TA
	`AWS::IAM::InstanceProfile`	TA	TA
	`AWS::IAM::OIDCProvider`	TA	TA
AWS Identity and Access Management Access Analyzer	`AWS::AccessAnalyzer::Analyzer`	TA	TA

AWS Config menyertakan kebijakan sebaris dengan detail konfigurasi yang direkam. Untuk informasi selengkapnya tentang kebijakan sebaris, lihat Kebijakan terkelola dan kebijakan sebaris di Panduan Pengguna IAM.

AWS IoT

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS IoT	`AWS::IoT::AccountAuditConfiguration`	TA	TA
	`AWS::IoT::Authorizer`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::IoT::CACertificate`	TA	TA
	`AWS::IoT::CustomMetric`	TA	TA
	`AWS::IoT::Dimension`	TA	TA
	`AWS::IoT::DomainConfiguration`	TA	TA
	`AWS::IoT::JobTemplate`	TA	TA
	`AWS::IoT::MitigationAction`	TA	TA
	`AWS::IoT::Policy`	TA	TA
	`AWS::IoT::ProvisioningTemplate`	TA	TA
	`AWS::IoT::RoleAlias`	TA	TA
	`AWS::IoT::ScheduledAudit`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::IoT::Security Profile`	TA	TA
	`AWS::IoTSiteWise::Gateway`	TA	TA
AWS IoT Wireless	`AWS::IoTWireless::ServiceProfile`	TA	TA
	`AWS::IoTWireless::MulticastGroup`	TA	TA
	`AWS::IoTWireless::FuotaTask`	TA	TA
AWS IoT Core	`AWS::IoT::FleetMetric`	TA	TA
AWS IoT Analytics	`AWS::IoTAnalytics::Datastore`	TA	TA
	`AWS::IoTAnalytics::Dataset`	TA	TA
	`AWS::IoTAnalytics::Pipeline`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::IoTAnalytics::Channel`	TA	TA
AWS IoT Events	`AWS::IoTEvents::Input`	TA	TA
	`AWS::IoTEvents::DetectorModel`	TA	TA
	`AWS::IoTEvents::AlarmModel`	TA	TA
AWS IoT TwinMaker	`AWS::IoTTwinMaker::Workspace`	TA	TA
	`AWS::IoTTwinMaker::Entity`	TA	TA
	`AWS::IoTTwinMaker::Scene`	TA	TA
	`AWS::IoTTwinMaker::SyncJob`	TA	TA
	`AWS::IoTTwinMaker::ComponentType`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS IoT SiteWise	`AWS::IoTSiteWise::Dashboard`	TA	TA
	`AWS::IoTSiteWise::Project`	TA	TA
	`AWS::IoTSiteWise::Portal`	TA	TA
	`AWS::IoTSiteWise::AssetModel`	TA	TA
AWS IoT Greengrass Version 2	`AWS::GreengrassV2::ComponentVersion`	TA	TA

AWS Key Management Service

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Key Management Service	`AWS::KMS::Key`	TA	TA
	`AWS::KMS::Alias`	TA	TA

AWS Lambda

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Lambda	`AWS::Lambda::Function`	dikaitkan dengan	Peran IAM
			EC2 kelompok keamanan
		terkandung dalam	EC2 subnet
	`AWS::Lambda::CodeSigningConfig`	TA	TA

AWS Mainframe Modernization

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Mainframe Modernization	`AWS::M2::Environment`	TA	TA

AWS Network Firewall

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Network Firewall	`AWS::NetworkFirewall::Firewall`	melekat pada	EC2 Subnet
		dikaitkan dengan	NetworkFirewall FirewallPolicy
	`AWS::NetworkFirewa`	dikaitkan dengan	NetworkFirewall RuleGroup

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`ll::FirewallPolicy`		
	`AWS::NetworkFirewall::RuleGroup`	TA	TA
	`AWS::NetworkFirewall::TLSInspectionConfiguration`	TA	TA
	`AWS::NetworkFirewall::VpcEndpointAssociation`	TA	TA

AWS Network Manager

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Network Manager	`AWS::NetworkManager::TransitGatewayRegistration`	TA	TA
	`AWS::NetworkManager::Site`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::NetworkManager::Device`	TA	TA
	`AWS::NetworkManager::Link`	TA	TA
	`AWS::NetworkManager::GlobalNetwork`	TA	TA
	`AWS::NetworkManager::CustomerGatewayAssociation`	TA	TA
	`AWS::NetworkManager::LinkAssociation`	TA	TA
	`AWS::NetworkManager::ConnectPeer`	TA	TA

AWS Panorama

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Panorama	`AWS::Panorama::Package`	TA	TA

AWS Private Certificate Authority

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Private Certificate Authority	`AWS::ACMPCA::CertificateAuthority`	TA	TA
	`AWS::ACMPCA::CertificateAuthorityActivation`	TA	TA
AWS Private CA Konektor untuk Active Directory	`AWS::PCAConnectorAD::DirectoryRegistration`	TA	TA

AWS Resilience Hub

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Resilience Hub	`AWS::ResilienceHub::ResiliencyPolicy`	TA	TA
	`AWS::ResilienceHub::App`	TA	TA

Penjelajah Sumber Daya AWS

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Penjelajah Sumber Daya AWS	`AWS::ResourceExplorer2::Index`	TA	TA

AWS RoboMaker

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS RoboMaker	`AWS::RoboMaker::RobotApplicationVersion`	TA	TA
	`AWS::RoboMaker::RobotApplication`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::RoboMaker::SimulationApplication`	TA	TA

AWS Signer

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Signer	`AWS::Signer::SigningProfile`	TA	TA

AWS Secrets Manager

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Secrets Manager	`AWS::SecretsManager::Secret`	dikaitkan dengan	Fungsi Lambda
		dikaitkan dengan	Kunci KMS

AWS Security Hub

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Security Hub	`AWS::SecurityHub::Standard`	TA	TA

AWS Service Catalog

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Service Catalog	`AWS::ServiceCatalog::CloudFormationProduct`	terkandung dalam	Portofolio
		dikaitkan dengan	CloudFormationProvisionedProduct
	`AWS::ServiceCatalog::CloudFormationProvisionedProduct`	dikaitkan dengan	Portofolio
			CloudFormationProduct
			CloudFormationStack
	`AWS::ServiceCatalog::Portfolio`	mengandung	CloudFormationProduct

> **Note**
>
> Saat Anda menggunakan AWS Service Catalog with AWS Config, item konfigurasi menampilkan ARN produk yang disediakan turunan, bukan ARN produk induk. Ini terjadi

ketika produk yang AWS Service Catalog disediakan berfungsi sebagai sumber daya dalam produk yang disediakan induk melalui. CloudFormation ID sumber daya tetap dapat dilacak melalui antarmuka. AWS Config

AWS Shield

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Shield	`AWS::Shield::Protection`	dikaitkan dengan	CloudFront Distribusi Amazon
	`AWS::ShieldRegional::Protection`	dikaitkan dengan	EC2 EIP
		dikaitkan dengan	ElasticLoadBalancing Penyeimbang
		dikaitkan dengan	ElasticLoadBalancingV2 LoadBalancer

AWS Step Functions

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Step Functions	`AWS::StepFunctions::Activity`	TA	TA
	`AWS::StepFunctions::StateMachine`	TA	TA

AWS Systems Manager

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Systems Manager	`AWS::SSM::ManagedInstanceInventory` *	dikaitkan dengan	EC2 contoh
	`AWS::SSM::PatchCompliance`	dikaitkan dengan	Inventaris Instance Terkelola
	`AWS::SSM::AssociationCompliance`	dikaitkan dengan	Inventaris Instance Terkelola
	`AWS::SSM::FileData`	dikaitkan dengan	Inventaris Instance Terkelola
	`AWS::SSM::Document`	TA	TA

* Untuk mempelajari lebih lanjut tentang inventaris instans terkelola, lihatRecording Software Configuration for Managed Instances.

AWS Transfer Family

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Transfer Family	`AWS::Transfer::Agreement`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::Transfer::Connector`	TA	TA
	`AWS::Transfer::Workflow`	TA	TA
	`AWS::Transfer::Certificate`	TA	TA
	`AWS::Transfer::Profile`	TA	TA

AWS WAF

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS WAF	`AWS::WAF::RateBasedRule`	TA	TA
	`AWS::WAF::Rule`	TA	TA
	`AWS::WAF::WebACL`	dikaitkan dengan	Aturan WAF
			Aturan berbasis tarif WAF
			Grup Aturan WAF
	`AWS::WAF::RuleGroup`	dikaitkan dengan	Aturan WAF

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::WAFRegional::RateBasedRule`	TA	TA
	`AWS::WAFRegional::Rule`	TA	TA
	`AWS::WAFRegional::WebACL`	dikaitkan dengan	ElasticLoadBalancingV2 LoadBalancer
			WAFRegional Aturan
			WAFRegional aturan berdasarkan tarif
			WAFRegional Grup aturan
	`AWS::WAFRegional::RuleGroup`	dikaitkan dengan	WAFRegional Aturan
AWS WAF V2	`AWS::WAFv2::WebACL`	dikaitkan dengan	ElasticLoadBalancingV2 LoadBalancer
			ApiGateway Panggung
			WAFv2 IPSet
			WAFv2 RegexPatternSet
			WAFv2 RuleGroup
			WAFv2 ManagedRuleSet

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::WAFv2::RuleGroup`	dikaitkan dengan	WAFv2 IPSet
			WAFv2 RegexPatternSet
	`AWS::WAFv2::ManagedRuleSet`	dikaitkan dengan	WAFv2 RuleGroup
	`AWS::WAFv2::IPSet`	TA	TA
	`AWS::WAFv2::RegexPatternSet`	TA	TA

AWS X-Ray

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS X-Ray	`AWS::XRay::EncryptionConfig`	TA	TA

Penyeimbang Beban Elastis

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
Penyeimbang Beban Elastis	Penyeimbang Beban Aplikasi	dikaitkan dengan	EC2 kelompok keamanan

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`AWS::ElasticLoadBalancingV2::LoadBalancer`	melekat pada	Subnet
		terkandung dalam	Cloud privat virtual (VPC)
	Pendengar Application Load Balancer `AWS::ElasticLoadBalancingV2::Listener`	TA	TA
	Classic Load Balancer `AWS::ElasticLoadBalancing::LoadBalancer`	dikaitkan dengan	EC2 kelompok keamanan
		melekat pada	Subnet
		terkandung dalam	Cloud privat virtual (VPC)
	Penyeimbang Beban Jaringan `AWS::ElasticLoadBalancingV2::LoadBalancer`	TA	TA

AWS Elemental MediaConnect

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Elemental MediaConnect	`AWS::MediaConnect::FlowEntitlement`	TA	TA
	`AWS::MediaConnect::FlowVpcInterface`	TA	TA
	`AWS::MediaConnect::FlowSource`	TA	TA
	`AWS::MediaConnect::Gateway`	TA	TA

AWS Elemental MediaPackage

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Elemental MediaPackage	`AWS::MediaPackage::PackagingGroup`	TA	TA
	`AWS::MediaPackage:`	TA	TA

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
	`:PackagingConfiguration`		

AWS Elemental MediaTailor

AWS Layanan	Nilai Jenis Sumber Daya	Hubungan	Sumber Daya Terkait
AWS Elemental MediaTailor	`AWS::MediaTailor::PlaybackConfiguration`	TA	TA

Cakupan Sumber Daya berdasarkan Ketersediaan Wilayah

Wilayah Amerika Utara dan Selatan

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::ACM::Certificate	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ACMPCA::CertificateAuthority	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::ACMPCA::CertificateAuthorityAktivasi	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::APS::RuleGroupsNamespace	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::AccessAnalyzer::Analyzer	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::AmazonMQ::Broker	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Amplify::App	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Amplify::Branch	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::ApiGateway::RestApi	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ApiGateway::Stage	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ApiGatewayV2::Api	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ApiGatewayV2::Stage	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::AppConfig::Application	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::AppConfig::ConfigurationProfile	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::AppConfig::DeploymentStrategy	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::AppConfig::Environment	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::AppConfig::ExtensionAssociation	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::AppConfig::HostedConfigurationVersi	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::AppFlow::Flow	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::AppIntegrations::Application	Tidak	Ya	Ya	Tidak	Tidak	Ya	Tidak	Tidak
AWS::AppIntegrations::EventIntegration	Tidak	Ya	Ya	Tidak	Tidak	Ya	Tidak	Tidak
AWS::AppMesh::GatewayRoute	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::AppMesh::Mesh	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::AppMesh::Route	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::AppMesh::VirtualGateway	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::AppMesh::VirtualNode	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::AppMesh::VirtualRouter	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::AppMesh::VirtualService	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::AppRunner::Service	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::AppRunner::VpcConnector	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::AppStream::Application	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::AppStream::DirectoryConfig	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::AppStream::Fleet	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::AppStream::Stack	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::AppSync::ApiCache	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::AppSync::GraphQLApi	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Athena::DataCatalog	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::Athena::PreparedStatement	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::Athena::WorkGroup	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::AuditManager::Assessment	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::AutoScaling::AutoScalingKelompok	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::AutoScaling::LaunchConfiguration	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::AutoScaling::ScalingPolicy	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::AutoScaling::ScheduledAction	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Auto Scaling::WarmPool	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Backup::BackupPlan	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::Backup::BackupSelection	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::Backup::BackupVault	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::Backup::RecoveryPoint	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::Backup::ReportPlan	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Batch::ComputeEnvironment	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Batch::JobQueue	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Batch::SchedulingPolicy	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::Bedrock::Guardrail	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Bedrock::KnowledgeBase	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Budgets::BudgetsAction	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Cassandra::Keyspace	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Cloud9::EnvironmentEC2	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::CloudFormation::Stack	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::CloudFront::Distribution	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::CloudFront::StreamingDistribution	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::CloudTrail::Trail	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::CloudWatch::Alarm	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::CloudWatch::MetricStream	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::CodeArtifact::Repository	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::CodeBuild::Project	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::CodeBuild::ReportGroup	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::CodeDeploy::Application	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::CodeDeploy::DeploymentConfig	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::CodeDeploy::DeploymentGroup	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::CodeGuruProfiler::ProfilingGroup	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::CodeGuruReviewer::RepositoryAssociation	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::CodePipeline::Pipeline	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Cognito::IdentityPool	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::Cognito::UserPool	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::Cognito::UserPoolKlien	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::Cognito::UserPoolKelompok	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::Config::ConfigurationRecorder	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Config::ConformancePackKepatuhan	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::Config::ResourceCompliance	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Connect::Instance	Tidak	Ya	Ya	Tidak	Tidak	Ya	Tidak	Tidak

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::Connect::PhoneNumber	Tidak	Ya	Ya	Tidak	Tidak	Ya	Tidak	Tidak
AWS::Connect::QuickConnect	Tidak	Ya	Ya	Tidak	Tidak	Ya	Tidak	Tidak
AWS::Connect::Rule	Tidak	Ya	Ya	Tidak	Tidak	Ya	Tidak	Tidak
AWS::Connect::User	Tidak	Ya	Ya	Tidak	Tidak	Ya	Tidak	Tidak
AWS::CustomerProfiles::Domain	Tidak	Ya	Ya	Tidak	Tidak	Ya	Tidak	Tidak
AWS::CustomerProfiles::ObjectType	Tidak	Ya	Ya	Tidak	Tidak	Ya	Tidak	Tidak
AWS::DMS::Certificate	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::DMS::Endpoint	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::DMS::EventSubscription	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::DMS::ReplicationInstance	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::DMS::ReplicationSubnetKelompok	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::DMS::ReplicationTask	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::DataSync::LocationEFS	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::DataSync::LocationFSxKilau	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::DataSync::LocationFSxJendela	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::DataSync::LocationHDFS	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::DataSync::LocationNFS	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::DataSync::LocationObjectPenyimpanan	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::DataSync::LocationS3	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::DataSync::LocationSMB	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::DataSync::Task	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::Detective::Graph	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::DeviceFarm::InstanceProfile	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::DeviceFarm::Project	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::DeviceFarm::TestGridProyek	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::DynamoDB::Table	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::Capacity Reservation	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::EC2::CarrierGateway	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::EC2::ClientVpnTitik akhir	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EC2::ClientVpnTargetNetworkAssociation	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EC2::CustomerGateway	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2:: DHCPOptions	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS:::EC2: EC2 Armada	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::EC2: :EIP	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2:: EIPAssociation	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::EgressOnlyInternetGateway	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EC2::FlowLog	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EC2::Host	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2: :IPAM	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EC2:: IPAMPool	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EC2:: IPAMResource Penemuan	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EC2:: IPAMResource DiscoveryAssociation	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EC2:: IPAMScope	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EC2::Instance	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::EC2::Instance ConnectTitik akhir	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::EC2::InternetGateway	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::LaunchTemplate	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EC2::NatGateway	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EC2::NetworkAcl	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::NetworkInsightsAccessScope	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EC2::NetworkInsightsAccessScopeAnalysis	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EC2::NetworkInsightsAnalisa	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EC2::NetworkInsightsJalan	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EC2::NetworkInterface	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::PrefixList	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::EC2::RegisteredHAInstance	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EC2::RouteTable	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::SecurityGroup	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::SnapshotBlockPublicAccess	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::EC2::SpotFleet	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::EC2::Subnet	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::SubnetRouteTableAssociation	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EC2::TrafficMirrorFilter	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::EC2::TrafficMirrorSesi	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EC2::TrafficMirrorTarget	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EC2::TransitGateway	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::EC2::TransitGatewayLampiran	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EC2::TransitGatewayConnect	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EC2::TransitGatewayMulticastDomain	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::EC2::TransitGatewayRouteTable	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EC2: :VPC	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2:: VPCBlockPublicAccessExclusion	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::EC2:: VPCBlockPublicAccessOptions	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::EC2:: VPCEndpoint	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2:: VPCEndpoint ConnectionNotification	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2:: VPCEndpoint Layanan	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2:: VPCPeering Koneksi	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::EC2:: VPNConnection	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2:: VPNConnection Rute	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::EC2:: VPNGateway	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::Volume	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ECR: :PublicRepository	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::ECR::PullThroughCacheRule	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::ECR::RegistryPolicy	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::ECR::Repository	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::ECS: :CapacityProvider	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::ECS::Cluster	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ECS::Service	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::ECS::TaskDefinition	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ECS::TaskSet	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EFS::AccessPoint	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::EFS::FileSystem	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::EKS::Addon	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EKS::Cluster	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EKS::FargateProfile	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EKS::IdentityProviderConfig	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EMR::SecurityConfiguration	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::ElasticBeanstalk::Application	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::ElasticBeanstalk::ApplicationVersion	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::ElasticBeanstalk::Environment	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::ElasticLoadBalancing::LoadBalancer	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ElasticLoadBalancingV2::Listener	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::ElasticLoadBalancingV2::LoadBalancer	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Elasticsearch::Domain	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EventSchemas::Discoverer	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EventSchemas::Registry	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EventSchemas::RegistryPolicy	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::EventSchemas::Schema	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Events::ApiDestination	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Events::Archive	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::Events::Connection	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Events::Endpoint	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Events::EventBus	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::Events::Rule	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Evidently::Launch	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::Evidently::Project	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::Evidently::Segment	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::FIS::ExperimentTemplate	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Forecast::Dataset	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::Forecast::DatasetGroup	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::FraudDetector::EntityType	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::FraudDetector::Label	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::FraudDetector::Outcome	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::FraudDetector::Variable	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::GlobalAccelerator::Accelerator	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::GlobalAccelerator::EndpointGroup	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::GlobalAccelerator::Listener	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Glue::Classifier	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::Glue::Job	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::Glue::MLTransform	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::Grafana::Workspace	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::GreengrassV2::ComponentVersion	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::GroundStation::Config	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Ya
AWS::GroundStation::DataflowEndpointKelompok	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Ya
AWS::GroundStation::MissionProfile	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Ya
AWS::GuardDuty::Detector	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::GuardDuty::Filter	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::GuardTugas:: IPSet	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::GuardDuty::ThreatIntelSet	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::HealthDanau::FHIRDatastore	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::IAM::Group	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::IAM::InstanceProfile	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS: :IAM:: OIDCProvider	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::IAM::Policy	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::IAM::Role	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS: :IAM:: SAMLProvider	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::IAM: :ServerCertificate	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::IAM::User	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::IVS::Channel	Tidak	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::IVS::Playback KeyPasangan	Tidak	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::IVS::RecordingConfiguration	Tidak	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::ImageBuilder: :ContainerRecipe	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::ImageBuilder: :DistributionConfiguration	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::ImageBuilder: :ImagePipeline	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::ImageBuilder::ImageRecipe	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::ImageBuilder::InfrastructureConfiguration	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::InspectorV2::Activation	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::InspectorV2::Filter	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::IoT::AccountAuditKonfigurasi	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::IoT::Authorizer	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::IoT:: CACertificate	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::IoT::CustomMetric	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::IoT::Dimension	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::IoT::FleetMetric	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::IoT::JobTemplate	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::IoT::MitigationAction	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::IoT::Policy	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::IoT::ProvisioningTemplate	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::IoT::RoleAlias	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::IoT::ScheduledAudit	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::IoT::SecurityProfile	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::IoTAnalytics::Channel	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::IoTAnalytics::Dataset	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::IoTAnalytics::Datastore	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::IoTAnalytics::Pipeline	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::IoTEvents::AlarmModel	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::IoTEvents::DetectorModel	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::IoTEvents::Input	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::IoTSiteWise::AssetModel	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::IoTSiteWise::Dashboard	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::IoTSiteWise::Gateway	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::IoTSiteWise::Portal	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::IoTSiteWise::Project	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::IoTTwinMaker::ComponentType	Tidak	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::IoTTwinMaker::Entity	Tidak	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::IoTTwinMaker::Scene	Tidak	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::IoTTwinMaker::SyncJob	Tidak	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::IoTTwinMaker::Workspace	Tidak	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::IoTWireless::FuotaTask	Tidak	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Ya
AWS::IoTWireless::MulticastGroup	Tidak	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Ya
AWS::IoTWireless::ServiceProfile	Tidak	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Ya
AWS::KMS::Alias	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::KMS::Key	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::KafkaConnect::Connector	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Kendra::Index	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::Kinesis::Stream	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Kinesis::StreamConsumer	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::KinesisAnalyticsV2::Application	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::KinesisFirehose::DeliveryStream	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::KinesisVideo::SignalingChannel	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::KinesisVideo::Stream	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Lambda::CodeSigningConfig	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Lambda::Function	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Lex::Bot	Tidak	Ya	Ya	Tidak	Tidak	Ya	Tidak	Tidak
AWS::Lex::BotAlias	Tidak	Ya	Ya	Tidak	Tidak	Ya	Tidak	Tidak
AWS::Lightsail::Bucket	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::Lightsail::Certificate	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::Lightsail::Disk	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::Lightsail::StaticIp	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::Logs::Destination	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::LookoutMetrics::Alert	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::LookoutVision::Project	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::M2::Environment	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::MSK::BatchScramRahasia	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::MSK::Cluster	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::MSK::ClusterPolicy	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::MSK::Configuration	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::MSK::VpcConnection	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Macie::Session	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::MediaConnect::FlowEntitlement	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::MediaConnect::FlowSource	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::MediaConnect::FlowVpcAntarmuka	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::MediaConnect::Gateway	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::MediaPackage::PackagingConfiguration	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::MediaPackage::PackagingGroup	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::MediaTailor::PlaybackConfiguration	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::MemoryDB::SubnetGroup	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::NetworkFirewall::Firewall	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::NetworkFirewall::FirewallPolicy	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::NetworkFirewall::RuleGroup	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::NetworkFirewall::TLSInspection Konfigurasi	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::NetworkFirewall::VpcEndpointAsosiasi	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::NetworkManager::ConnectPeer	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::NetworkManager::CustomerGatewayAsosiasi	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::NetworkManager::Device	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::NetworkManager::GlobalNetwork	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::NetworkManager::Link	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::NetworkManager::LinkAssociation	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::NetworkManager::Site	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::NetworkManager::TransitGatewayRegistrasi	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::OpenSearch::Domain	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::OpenSearchServerless::Collection	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::OpenSearchServerless::VpcEndpoint	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Panorama::Package	Tidak	Ya	Ya	Tidak	Tidak	Ya	Tidak	Tidak
AWS::Personalize::Dataset	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::Personalize::DatasetGroup	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::Personalize::Schema	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::Personalize::Solution	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::Pinpoint::App	Tidak	Ya	Ya	Tidak	Tidak	Ya	Tidak	Tidak
AWS::Pinpoint::ApplicationSettings	Tidak	Ya	Ya	Tidak	Tidak	Ya	Tidak	Tidak
AWS::Pinpoint::Campaign	Tidak	Ya	Ya	Tidak	Tidak	Ya	Tidak	Tidak
AWS::Pinpoint::EmailChannel	Tidak	Ya	Ya	Tidak	Tidak	Ya	Tidak	Tidak
AWS::Pinpoint::EmailTemplate	Tidak	Ya	Ya	Tidak	Tidak	Ya	Tidak	Tidak

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::Pinpoint::EventStream	Tidak	Ya	Ya	Tidak	Tidak	Ya	Tidak	Tidak
AWS::Pinpoint::InAppTemplate	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::Pinpoint::Segment	Tidak	Ya	Ya	Tidak	Tidak	Ya	Tidak	Tidak
AWS::QLDB::Ledger	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::QuickSight::DataSource	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::QuickSight::Template	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::QuickSight::Theme	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS: :RDS:: DBCluster	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS: :RDS:: Snapshot DBCluster	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS: :RDS:: DBInstance	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS: :RDS:: Grup DBSecurity	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS: :RDS:: DBSnapshot	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS: :RDS:: Grup DBSubnet	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::RDS: :EventSubscription	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::RDS::GlobalCluster	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::RDS::OptionGroup	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::RUM::AppMonitor	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Redshift::Cluster	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Redshift::ClusterParameterKelompok	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Redshift::ClusterSecurityKelompok	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Redshift::ClusterSnapshot	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Redshift::ClusterSubnetKelompok	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::Redshift::EndpointAccess	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Redshift::EndpointAuthorization	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Redshift::EventSubscription	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Redshift::ScheduledAction	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::ResilienceHub::App	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::ResilienceHub::ResiliencyPolicy	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::ResourceExplorer2::Index	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::RoboMaker::RobotApplication	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::RoboMaker::RobotApplicationVersi	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::RoboMaker::SimulationApplication	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::Route53::HealthCheck	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::Route53::HostedZone	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Route53Profiles::Profile	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::Route53RecoveryControl::Cluster	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Route53RecoveryControl::ControlPanel	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Route53RecoveryControl::RoutingControl	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Route53RecoveryControl::SafetyRule	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Route53RecoveryReadiness::Cell	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Route53RecoveryReadiness::ReadinessCheck	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Route53RecoveryReadiness::RecoveryGroup	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Route53RecoveryReadiness::ResourceSet	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Route53Resolver::FirewallDomainDaftar	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::Route53Resolver::FirewallRuleKelompok	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Route53Resolver::FirewallRuleGroupAssociation	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Route53Resolver::ResolverEndpoint	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Route53Resolver::ResolverQueryLoggingConfig	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Route53Resolver::ResolverRule	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Route53Resolver::ResolverRuleAsosiasi	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::S3::AccessPoint	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::S3::AccountPublicAccessBlock	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::S3::Bucket	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::S3::MultiRegionAccessPoint	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::S3::StorageLens	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::S3::StorageLensKelompok	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::S3Express::BucketPolicy	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::S3Express::DirectoryBucket	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::SES::ConfigurationSet	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::SES::ContactList	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::SES::ReceiptFilter	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::SES::ReceiptRuleSet	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::SES::Template	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::SNS::Topic	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::SQS::Queue	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::SSM::AssociationCompliance	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::SSM::Document	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::SSM::FileData	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::SSM::ManagedInstanceInventaris	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::SSM::PatchCompliance	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::SageMaker::AppImageConfig	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::SageMaker::CodeRepository	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::SageMaker::Domain	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::SageMaker::EndpointConfig	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::SageMaker::FeatureGroup	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::SageMaker::Image	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::SageMaker::InferenceExperiment	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::SageMaker::Model	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::SageMaker::NotebookInstance	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::SageMaker::NotebookInstanceLifecycleConfig	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::SageMaker::Workteam	Tidak	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
AWS::SecretsManager::Secret	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::SecurityHub::Standard	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ServiceCatalog::CloudFormationProduk	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::ServiceCatalog::Portfolio	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::ServiceDiscovery::HttpNamespace	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::ServiceDiscovery::Instance	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::ServiceDiscovery::PublicDnsNamespace	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::ServiceDiscovery::Service	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Shield::Protection	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::ShieldRegional::Protection	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Signer::SigningProfile	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Step Functions::Activity	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::StepFunctions::StateMachine	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::Transfer::Agreement	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::Transfer::Certificate	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::Transfer::Connector	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::Transfer::Profile	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::Transfer::Workflow	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::WAF::RateBasedAturan	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::WAF::Rule	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::WAF::RuleGroup	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::WAF::WebACL	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::WAFRegional::RateBasedAturan	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::WAFRegional::Rule	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::WAFRegional::RuleGroup	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya
AWS::WAFRegional::WebACL	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya

Jenis sumber daya	AS Barat (California N.)	AS Timur (Virginia N.)	AS Barat (Oregon)	AS Timur (Ohio)	Kanada Barat (Calgary)	Kanada (Tengah)	Meksiko (Tengah)	Amerika Selatan (São Paulo)
AWS::WAFv2:: IPSet	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::WAFv 2::ManagedRuleSet	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::WAFv 2::RegexPatternSet	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::WAFv2::RuleGroup	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::WAFv2::WebACL	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::WorkSpaces::C onnectionAlias	Tidak	Ya	Ya	Tidak	Tidak	Ya	Tidak	Ya
AWS::Work Spaces::Workspace	Tidak	Ya	Ya	Tidak	Tidak	Ya	Tidak	Ya
AWS::XRay ::EncryptionConfig	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak	Ya

Wilayah Eropa

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::ACM::Certificate	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ACMPCA::CertificateAuthority	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ACMPCA::CertificateAuthorityAktivasi	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::APS::RuleGroupsNamespace	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::AccessAnalyzer::Analyzer	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::AmazonMQ::Broker	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::Amplify::App	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::Amplify::Branch	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::ApiGateway::RestApi	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ApiGateway::Stage	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ApiGatewayV2::Api	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::ApiGatewayV2::Stage	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::AppConfig::Application	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::AppConfig::ConfigurationProfile	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::AppConfig::DeploymentStrategy	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::AppConfig::Environment	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::AppConfig::ExtensionAssociation	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::AppConfig::HostedConfigurationVersi	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::AppFlow::Flow	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::AppIntegrations::Application	Tidak	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::AppIntegrations::EventIntegration	Tidak	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::AppMesh::GatewayRoute	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::AppMesh::Mesh	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::AppMesh::Route	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::AppMesh::VirtualGateway	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::AppMesh::VirtualNode	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::AppMesh::VirtualRouter	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::AppMesh::VirtualService	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::AppRunner::Service	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::AppRunner::VpcConnector	Ya	Ya	Tidak	Ya	Tidak	Tidak	Tidak	Tidak
AWS::AppStream::Application	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::AppStream::DirectoryConfig	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::AppStream::Fleet	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::AppStream::Stack	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::AppSync::ApiCache	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::AppSync::GraphQLApi	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Athena::DataCatalog	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Athena::PreparedStatement	Ya	Ya	Ya	Ya	Ya	Tidak	Ya	Ya
AWS::Athena::WorkGroup	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::AuditManager::Assessment	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::AutoScaling::AutoScalingKelompok	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::AutoScaling::LaunchConfiguration	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::AutoScaling::ScalingPolicy	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::AutoScaling::ScheduledAction	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::Auto Scaling::WarmPool	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::Backup::BackupPlan	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Backup::BackupSelection	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Backup::BackupVault	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Backup::RecoveryPoint	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Backup::ReportPlan	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::Batch::ComputeEnvironment	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Batch::JobQueue	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Batch::SchedulingPolicy	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Bedrock::Guardrail	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Bedrock::KnowledgeBase	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::Cassandra::Keyspace	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::Cloud9::EnvironmentEC2	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::CloudFormation::Stack	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::CloudTrail::Trail	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::CloudWatch::Alarm	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::CloudWatch::MetricStream	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::CodeArtifact::Repository	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::CodeBuild::Project	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::CodeBuild::ReportGroup	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::CodeDeploy::Application	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::CodeDeploy::DeploymentConfig	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::CodeDeploy::DeploymentGroup	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::CodeGuruProfiler::ProfilingGroup	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak	Tidak
AWS::CodeGuruReviewer::RepositoryAssociation	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak	Tidak
AWS::CodePipeline::Pipeline	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Cognito::IdentityPool	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Cognito::UserPool	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Cognito::UserPoolKlien	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Cognito::UserPoolKelompok	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Config::ConfigurationRecorder	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Config::ConformancePackKepatuhan	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Config::ResourceCompliance	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::Connect::Instance	Tidak	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Connect::PhoneNumber	Tidak	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Connect::QuickConnect	Tidak	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Connect::Rule	Tidak	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Connect::User	Tidak	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::CustomerProfiles::Domain	Tidak	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::CustomerProfiles::ObjectType	Tidak	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::DMS::Certificate	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::DMS::Endpoint	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::DMS::EventSubscription	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::DMS::ReplicationInstance	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::DMS::ReplicationSubnetKelompok	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::DMS::ReplicationTask	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::DataSync::LocationEFS	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::DataSync::LocationFSxKilau	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::DataSync::LocationFSxJendela	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::DataSync::LocationHDFS	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::DataSync::LocationNFS	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::DataSync::LocationObjectPenyimpanan	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::DataSync::LocationS3	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::DataSync::LocationSMB	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::DataSync::Task	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::Detective::Graph	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::DynamoDB::Table	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::Capacity Reservation	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::CarrierGateway	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::EC2: :ClientVpnTitik akhir	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::EC2::ClientVpnTargetNetworkAssociation	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::EC2: :CustomerGateway	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2:: DHCPOptions	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS:::EC2: EC2 Armada	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2: :EIP	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2:: EIPAssociation	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::EC2::EgressOnlyInternetGateway	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::EC2::FlowLog	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::EC2::Host	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2: :IPAM	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2:: IPAMPool	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2:: IPAMResource Penemuan	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2:: IPAMResource DiscoveryAssociation	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2:: IPAMScope	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::Instance	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::InstanceConnectTitik akhir	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2: :InternetGateway	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::EC2::LaunchTemplate	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::EC2::NatGateway	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::EC2::NetworkAcl	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::NetworkInsightsAccessScope	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::EC2::NetworkInsightsAccessScopeAnalysis	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::EC2::NetworkInsightsAnalisa	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::EC2::NetworkInsightsJalan	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::EC2::NetworkInterface	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::PrefixList	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::RegisteredHAInstance	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::EC2::RouteTable	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::EC2::SecurityGroup	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::SnapshotBlockPublicAccess	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::SpotFleet	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::Subnet	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::SubnetRouteTableAssociation	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::TrafficMirrorFilter	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::TrafficMirrorSesi	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::TrafficMirrorTarget	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::EC2::TransitGateway	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::TransitGatewayLampiran	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::TransitGatewayConnect	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::EC2::TransitGatewayMulticastDomain	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::TransitGatewayRouteTable	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::EC2: :VPC	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2:: VPCBlockPublicAccessExclusion	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2:: VPCBlockPublicAccessOptions	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2:: VPCEndpoint	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2:: VPCEndpoint ConnectionNotification	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2:: VPCEndpoint Layanan	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2:: VPCPeering Koneksi	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2:: VPNConnection	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2:: VPNConnection Rute	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::EC2:: VPNGateway	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::Volume	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ECR::PullThroughCacheRule	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ECR::RegistryPolicy	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ECR::Repository	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ECS::CapacityProvider	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ECS::Cluster	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ECS::Service	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ECS::TaskDefinition	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ECS::TaskSet	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EFS::AccessPoint	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::EFS::FileSystem	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EKS::Addon	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EKS::Cluster	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EKS::FargateProfile	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EKS::IdentityProviderConfig	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EMR::SecurityConfiguration	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ElasticBeanstalk::Application	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::ElasticBeanstalk::ApplicationVersion	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::ElasticBeanstalk::Environment	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::ElasticLoadBalancing::LoadBalancer	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ElasticLoadBalancingV2::Listener	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::ElasticLoadBalancingV2::LoadBalancer	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Elasticsearch::Domain	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EventSchemas::Discoverer	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EventSchemas::Registry	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EventSchemas::RegistryPolicy	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EventSchemas::Schema	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Events::ApiDestination	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Events::Archive	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Events::Connection	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Events::Endpoint	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::Events::EventBus	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::Events::Rule	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Evidently::Launch	Ya	Ya	Tidak	Tidak	Ya	Tidak	Tidak	Tidak
AWS::Evidently::Project	Ya	Ya	Tidak	Tidak	Ya	Tidak	Tidak	Tidak
AWS::Evidently::Segment	Ya	Ya	Tidak	Tidak	Ya	Tidak	Tidak	Tidak
AWS::FIS::ExperimentTemplate	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Tidak
AWS::Forecast::Dataset	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Forecast::DatasetGroup	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::FraudDetector::EntityType	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::FraudDetector::Label	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::FraudDetector::Outcome	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::FraudDetector::Variable	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::Glue::Classifier	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Glue::Job	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Glue::MLTransform	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Grafana::Workspace	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::GreengrassV2::ComponentVersion	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::GroundStation::Config	Ya	Ya	Tidak	Tidak	Ya	Tidak	Tidak	Tidak
AWS::GroundStation::DataflowEndpointKelompok	Ya	Ya	Tidak	Tidak	Ya	Tidak	Tidak	Tidak
AWS::GroundStation::MissionProfile	Ya	Ya	Tidak	Tidak	Ya	Tidak	Tidak	Tidak
AWS::GuardDuty::Detector	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::GuardDuty::Filter	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::GuardTugas:: IPSet	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::GuardDuty::ThreatIntelSet	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::IAM::Group	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::IAM::Policy	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::IAM::Role	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::IAM::User	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::IVS::Channel	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::IVS::PlaybackKeyPasangan	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::IVS::RecordingConfiguration	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::ImageBuilder::ContainerRecipe	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ImageBuilder::DistributionConfiguration	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ImageBuilder::ImagePipeline	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::ImageBuilder::ImageRecipe	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ImageBuilder::InfrastructureConfiguration	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::InspectorV2::Activation	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::InspectorV2::Filter	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::IoT::AccountAuditKonfigurasi	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::IoT::Authorizer	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::IoT:: CACertificate	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::IoT::CustomMetric	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::IoT::Dimension	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::IoT::FleetMetric	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::IoT::JobTemplate	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::IoT::MitigationAction	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::IoT::Policy	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::IoT::ProvisioningTemplate	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::IoT::RoleAlias	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::IoT::ScheduledAudit	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::IoT::SecurityProfile	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::IoTAnalytics::Channel	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::IoTAnalytics::Dataset	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::IoTAnalytics::Datastore	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::IoTAnalytics::Pipeline	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::IoTEvents::AlarmModel	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::IoTEvents::DetectorModel	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::IoTEvents::Input	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::IoTSiteWise::AssetModel	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::IoTSiteWise::Dashboard	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::IoTSiteWise::Gateway	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::IoTSiteWise::Portal	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::IoTSiteWise::Project	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::IoTTwinMaker::ComponentType	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::IoTTwinMaker::Entity	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::IoTTwinMaker::Scene	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::IoTTwinMaker::SyncJob	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::IoTTwinMaker::Workspace	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::IoTWireless::FuotaTask	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::IoTWireless::MulticastGroup	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::IoTWireless::ServiceProfile	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::KMS::Alias	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::KMS::Key	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::KafkaConnect::Connector	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::Kendra::Index	Ya	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Kinesis::Stream	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Kinesis::StreamConsumer	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::KinesisAnalyticsV2::Application	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::KinesisFirehose::DeliveryStream	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::KinesisVideo::SignalingChannel	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::KinesisVideo::Stream	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::Lambda::CodeSigningConfig	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::Lambda::Function	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Lex::Bot	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Lex::BotAlias	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Lightsail::Bucket	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::Lightsail::Certificate	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::Lightsail::Disk	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::Lightsail::StaticIp	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::Logs::Destination	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::LookoutMetrics::Alert	Ya	Ya	Tidak	Tidak	Ya	Tidak	Tidak	Tidak
AWS::LookoutVision::Project	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::M2::Environment	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::MSK::BatchScramRahasia	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::MSK::Cluster	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::MSK::ClusterPolicy	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::MSK::Configuration	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::MSK::VpcConnection	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Macie::Session	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::MediaConnect::FlowEntitlement	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::MediaConnect::FlowSource	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::MediaConnect::FlowVpcAntarmuka	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::MediaConnect::Gateway	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::MediaPackage::PackagingConfiguration	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::MediaPackage::PackagingGroup	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::MediaTailor::PlaybackConfiguration	Ya	Ya	Tidak	Ya	Ya	Tidak	Tidak	Tidak
AWS::MemoryDB::SubnetGroup	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak	Tidak
AWS::NetworkFirewall::Firewall	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::NetworkFirewall::FirewallPolicy	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::NetworkFirewall::RuleGroup	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::NetworkFirewall::TLSInspection Konfigurasi	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::NetworkFirewall::VpcEndpointAsosiasi	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::OpenSearch::Domain	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::OpenSearchServerless::Collection	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::OpenSearchServerless::VpcEndpoint	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak
AWS::Panorama::Package	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Personalize::Dataset	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Personalize::DatasetGroup	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Personalize::Schema	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Personalize::Solution	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Pinpoint::App	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Pinpoint::ApplicationSettings	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::Pinpoint::Campaign	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Pinpoint::EmailChannel	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Pinpoint::EmailTemplate	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Pinpoint::EventStream	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Pinpoint::InAppTemplate	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Pinpoint::Segment	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::QLDB::Ledger	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::QuickSight::DataSource	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::QuickSight::Template	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::QuickSight::Theme	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS: :RDS:: DBCluster	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS: :RDS:: Snapshot DBCluster	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS: :RDS:: DBInstance	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS: :RDS:: Grup DBSecurity	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS: :RDS:: DBSnapshot	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS: :RDS:: Grup DBSubnet	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::RDS: :EventSubscription	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::RDS::GlobalCluster	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::RDS::OptionGroup	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::RUM::AppMonitor	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Redshift::Cluster	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Redshift::ClusterParameterKelompok	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::Redshift::ClusterSecurityKelompok	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Redshift::ClusterSnapshot	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Redshift::ClusterSubnetKelompok	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Redshift::EndpointAccess	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::Redshift::EndpointAuthorization	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::Redshift::EventSubscription	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Redshift::ScheduledAction	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::ResilienceHub::App	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::ResilienceHub::ResiliencyPolicy	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::ResourceExplorer2::Index	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::RoboMaker::RobotApplication	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::RoboMaker::RobotApplicationVersi	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::RoboMaker::SimulationApplication	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::Route53Profiles::Profile	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Route53Resolver::FirewallDomainDaftar	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::Route53Resolver::FirewallRuleKelompok	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::Route53Resolver::FirewallRuleGroupAssociation	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::Route53Resolver::ResolverEndpoint	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Route53Resolver::ResolverQueryLoggingConfig	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::Route53Resolver::ResolverRule	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::Route53Resolver::ResolverRuleAsosiasi	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::S3::AccessPoint	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::S3::AccountPublicAccessBlock	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::S3::Bucket	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::S3::StorageLens	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::S3::StorageLensKelompok	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::S3Express::BucketPolicy	Ya	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	Tidak
AWS::S3Express::DirectoryBucket	Ya	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	Tidak
AWS::SES::ConfigurationSet	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::SES::ContactList	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::SES::ReceiptFilter	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::SES::ReceiptRuleSet	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::SES::Template	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::SNS::Topic	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::SQS::Queue	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::SSM::AssociationCompliance	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::SSM::Document	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::SSM::FileData	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::SSM::ManagedInstanceInventaris	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::SSM::PatchCompliance	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::SageMaker::AppImageConfig	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Tidak
AWS::SageMaker::CodeRepository	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::SageMaker::Domain	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::SageMaker::EndpointConfig	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::SageMaker::FeatureGroup	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Tidak
AWS::SageMaker::Image	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Tidak
AWS::SageMaker::InferenceExperiment	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::SageMaker::Model	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::SageMaker::NotebookInstance	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::SageMaker::NotebookInstanceLifecycleConfig	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::SageMaker::Workteam	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::SecretsManager::Secret	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::SecurityHub::Standard	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::ServiceCatalog::CloudFormationProduk	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ServiceCatalog::Portfolio	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ServiceDiscovery::HttpNamespace	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ServiceDiscovery::Instance	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::ServiceDiscovery::PublicDnsNamespace	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ServiceDiscovery::Service	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::ShieldRegional::Protection	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::Signer::SigningProfile	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::StepFunctions::Activity	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::StepFunctions::StateMachine	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::Transfer::Agreement	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak
AWS::Transfer::Certificate	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Transfer::Connector	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Transfer::Profile	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Transfer::Workflow	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::WAFRegional:: RateBasedAturan	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::WAFRegional::Rule	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::WAFRegional::RuleGroup	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::WAFRegional::WebACL	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::WAFv2:: IPSet	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::WAFv2::ManagedRuleSet	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	Eropa (Irlandia)	Eropa (Frankfurt am Main)	Eropa (London)	Eropa (Paris)	Eropa (Stockholm)	Eropa (Milan)	Eropa (Spanyol)	Eropa (Zürich)
AWS::WAFv2::RegexPatternSet	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::WAFv2::RuleGroup	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::WAFv2::WebACL	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::WorkSpaces::ConnectionAlias	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::WorkSpaces::Workspace	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::XRay::EncryptionConfig	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Wilayah Asia Pasifik

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::ACM::Certificate	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ACMPCA::CertificateAuthority	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::ACMPCA::CertificateAuthorityAktivasi	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::APS::RuleGroupsNamespace	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::AccessAnalyzer::Analyzer	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::AmazonMQ::Broker	Ya	Tidak	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Amplify::App	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Amplify::Branch	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::ApiGateway::RestApi	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya	Ya
AWS::ApiGateway::Stage	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya	Ya
AWS::ApiGatewayV2::Api	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya	Ya
AWS::ApiGatewayV2::Stage	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::AppConfig::Application	Ya	Tidak	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::AppConfig::ConfigurationProfile	Ya	Tidak	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::AppConfig::DeploymentStrategy	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::AppConfig::Environment	Ya	Tidak	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::AppConfig::ExtensionAssociation	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::AppConfig::HostedConfigurationVersi	Ya	Tidak	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::AppFlow::Flow	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::AppIntegrations::Application	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::AppIntegrations::EventIntegration	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::AppMesh::GatewayRoute	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::AppMesh::Mesh	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::AppMesh::Route	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::AppMesh::VirtualGateway	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::AppMesh::VirtualNode	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::AppMesh::VirtualRouter	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::AppMesh::VirtualService	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::AppRunner::Service	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	Ya	Ya	Tidak	Tidak	Ya
AWS::AppRunner::VpcConnector	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	Ya	Ya	Tidak	Tidak	Ya
AWS::AppStream::Application	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::AppStream::DirectoryConfig	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::AppStream::Fleet	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::AppStream::Stack	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::AppSync::ApiCache	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::AppSync::GraphQLApi	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Athena::DataCatalog	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Athena::PreparedStatement	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Athena::WorkGroup	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::AuditManager::Assessment	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	Ya	Ya	Tidak	Tidak	Ya
AWS::AutoScaling::AutoScalingKelompok	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::Auto Scaling:: LaunchConfiguration	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Auto Scaling:: ScalingPolicy	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Auto Scaling:: ScheduledAction	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Auto Scaling:: WarmPool	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Backup::BackupPlan	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Backup::BackupSelection	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Backup::BackupVault	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Backup::RecoveryPoint	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Backup::ReportPlan	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::Batch::ComputeEnvironment	Ya	Ya	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Batch::JobQueue	Ya	Ya	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Batch::SchedulingPolicy	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Bedrock::Guardrail	Tidak	Ya	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::Bedrock::KnowledgeBase	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Ya	Tidak	Ya
AWS::Cassandra::Keyspace	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Cloud9::EnvironmentEC2	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::CloudFormation::Stack	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::CloudTrail::Trail	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::CloudWatch::Alarm	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::CloudWatch::MetricStream	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::CodeArtifact::Repository	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	Ya	Ya	Tidak	Tidak	Ya
AWS::CodeBuild::Project	Ya	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::CodeBuild::ReportGroup	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::CodeDeploy::Application	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::CodeDeploy::DeploymentConfig	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::CodeDeploy::DeploymentGroup	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::CodeGuruProfiler::ProfilingGroup	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::CodeGuruReviewer::RepositoryAssociation	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Tidak	Tidak	Ya
AWS::CodePipeline::Pipeline	Ya	Ya	Tidak	Tidak	Ya	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Cognito::IdentityPool	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Cognito::UserPool	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Cognito::UserPoolKlien	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Cognito::UserPoolKelompok	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Config::ConfigurationRecorder	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Config::ConformancePackKepatuhan	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Config::ResourceCompliance	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::Connect::Instance	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Connect::PhoneNumber	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Connect::QuickConnect	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Connect::Rule	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Connect::User	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::CustomerProfiles::Domain	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::CustomerProfiles::ObjectType	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::DMS::Certificate	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::DMS::Endpoint	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::DMS::EventSubscription	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::DMS::ReplicationInstance	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::DMS::ReplicationSubnetKelompok	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::DMS::ReplicationTask	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::DataSync::LocationEFS	Ya	Tidak	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::DataSync::LocationFSxKilau	Ya	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::DataSync::LocationFSxJendela	Ya	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::DataSync::LocationHDFS	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::DataSync::LocationNFS	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::DataSync::LocationObjectPenyimpanan	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::DataSync::LocationS3	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::DataSync::LocationSMB	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::DataSync::Task	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Detective::Graph	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::DynamoDB::Table	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::Capacity Reservation	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::CarrierGateway	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Tidak	Tidak	Ya
AWS::EC2::ClientVpnTitik akhir	Ya	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::EC2::ClientVpnTargetNetworkAssociation	Ya	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::CustomerGateway	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::DHCPOptions	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS:::EC2:EC2 Armada	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2: :EIP	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::EIPAssociation	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya	Ya
AWS::EC2::EgressOnlyInternetGateway	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::FlowLog	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::Host	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2: :IPAM	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::EC2::IPAMPool	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::IPAMResource Penemuan	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::IPAMResource Discovery Association	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::IPAMScope	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::Instance	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::InstanceConnectTitik akhir	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::InternetGateway	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::LaunchTemplate	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::NatGateway	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::NetworkAcl	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::EC2::NetworkInsightsAccessScope	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::NetworkInsightsAccessScopeAnalysis	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::NetworkInsightsAnalisa	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::NetworkInsightsJalan	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::NetworkInterface	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::PrefixList	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::RegisteredHAInstance	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::RouteTable	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::SecurityGroup	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::EC2::SnapshotBlockPublicAccess	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::SpotFleet	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::Subnet	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::SubnetRouteTableAssociation	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::TrafficMirrorFilter	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::TrafficMirrorSesi	Ya	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::TrafficMirrorTarget	Ya	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::TransitGateway	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::TransitGatewayLampiran	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::EC2::TransitGatewayConnect	Ya	Tidak	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::TransitGatewayMulticastDomain	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::TransitGatewayRouteTable	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2: :VPC	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2:: VPCBlockPublicAccessExclusion	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2:: VPCBlockPublicAccessOptions	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::VPCEndpoint	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::EC2::VPCEndpointConnectionNotification	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya	Ya
AWS::EC2::VPCEndpoint Layanan	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::VPCPeering Koneksi	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::VPNConnection	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::VPNConnection Rute	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EC2::VPNGateway	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EC2::Volume	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ECR::PullThroughCacheRule	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::ECR::RegistryPolicy	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::ECR::Repository	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::ECS::CapacityProvider	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::ECS::Cluster	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ECS::Service	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ECS::TaskDefinition	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ECS::TaskSet	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EFS::AccessPoint	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EFS::FileSystem	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EKS::Addon	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EKS::Cluster	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EKS::FargateProfile	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::EKS::IdentityProviderConfig	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EMR::SecurityConfiguration	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::ElasticBeanstalk::Application	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::ElasticBeanstalk::ApplicationVersion	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::ElasticBeanstalk::Environment	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::ElasticLoadBalancing::LoadBalancer	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::ElasticLoadBalancingV2::Listener	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::ElasticLoadBalancingV2::LoadBalancer	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::Elasticsearch::Domain	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::EventSchemas::Discoverer	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EventSchemas::Registry	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EventSchemas::RegistryPolicy	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::EventSchemas::Schema	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Events::ApiDestination	Ya	Ya	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Events::Archive	Ya	Ya	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Events::Connection	Ya	Ya	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Events::Endpoint	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Events::EventBus	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::Events::Rule	Ya	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Evidently::Launch	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Tidak	Tidak	Ya
AWS::Evidently::Project	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Tidak	Tidak	Ya
AWS::Evidently::Segment	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Tidak	Tidak	Ya
AWS::FIS::ExperimentTemplate	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Forecast::Dataset	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Forecast::DatasetGroup	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::FraudDetector::EntityType	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Tidak	Tidak	Tidak
AWS::FraudDetector::Label	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Tidak	Tidak	Tidak
AWS::FraudDetector::Outcome	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Tidak	Tidak	Tidak

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::FraudDetector::Variable	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Tidak	Tidak	Tidak
AWS::Glue::Classifier	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Glue::Job	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Glue::MLTransform	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Grafana::Workspace	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::GreengrassV2::ComponentVersion	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::GroundStation::Config	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::GroundStation::DataflowEndpointKelompok	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak
AWS::GroundStation::MissionProfile	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::GuardDuty::Detector	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::GuardDuty::Filter	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::GuardTugas:: IPSet	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::GuardDuty::ThreatIntelSet	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::HealthDanau:: FHIRDatastore	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
AWS::IAM::Group	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::IAM::Policy	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::IAM::Role	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::IAM::User	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::IVS::Channel	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::IVS::PlaybackKeyPasangan	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Ya
AWS::IVS::RecordingConfiguration	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Ya
AWS::ImageBuilder::ContainerRecipe	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::ImageBuilder::DistributionConfiguration	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::ImageBuilder::ImagePipeline	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::ImageBuilder::ImageRecipe	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::ImageBuilder::InfrastructureConfiguration	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::InspectorV2::Activation	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::InspectorV2::Filter	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::IoT::AccountAuditKonfigurasi	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::IoT::Authorizer	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::IoT::CACertificate	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::IoT::CustomMetric	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::IoT::Dimension	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::IoT::FleetMetric	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::IoT::JobTemplate	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::IoT::MitigationAction	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::IoT::Policy	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::IoT::ProvisioningTemplate	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::IoT::RoleAlias	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::IoT::ScheduledAudit	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::IoT::SecurityProfile	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::IoTAnalytics::Channel	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	Ya
AWS::IoTAnalytics::Dataset	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	Ya
AWS::IoTAnalytics::Datastore	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	Ya
AWS::IoTAnalytics::Pipeline	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	Ya
AWS::IoTEvents::AlarmModel	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::IoTEvents::DetectorModel	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::IoTEvents::Input	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::IoTSiteWise::AssetModel	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::IoTSiteWise::Dashboard	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::IoTSiteWise::Gateway	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::IoTSiteWise::Portal	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::IoTSiteWise::Project	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::IoTTwinMaker::ComponentType	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::IoTTwinMaker::Entity	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Tidak	Tidak	Tidak
AWS::IoTTwinMaker::Scene	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::IoTTwinMaker::SyncJob	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::IoTTwinMaker::Workspace	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::IoTWireless::FuotaTask	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	Ya
AWS::IoTWireless::MulticastGroup	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	Ya
AWS::IoTWireless::ServiceProfile	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	Ya
AWS::KMS::Alias	Ya	Ya	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::KMS::Key	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::KafkaConnect::Connector	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Kendra::Index	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	Ya	Ya	Tidak	Tidak	Ya
AWS::Kinesis::Stream	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Kinesis::StreamConsumer	Ya	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::KinesisAnalyticsV2::Application	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::KinesisFirehose::DeliveryStream	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::KinesisVideo::SignalingChannel	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::KinesisVideo::Stream	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Lambda::CodeSigningConfig	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Lambda::Function	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Lex::Bot	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Lex::BotAlias	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Lightsail::Bucket	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Lightsail::Certificate	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Lightsail::Disk	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::Lightsail::StaticIp	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Logs::Destination	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::LookoutMetrics::Alert	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Tidak	Tidak	Ya
AWS::LookoutVision::Project	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Ya
AWS::M2::Environment	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::MSK::BatchScramRahasia	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::MSK::Cluster	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::MSK::ClusterPolicy	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::MSK::Configuration	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::MSK::VpcConnection	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Macie::Session	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::MediaConnect::FlowEntitlement	Ya	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::MediaConnect::FlowSource	Ya	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::MediaConnect::FlowVpcAntarmuka	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::MediaConnect::Gateway	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::MediaPackage::PackagingConfiguration	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::MediaPackage::PackagingGroup	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::MediaTailor::PlaybackConfiguration	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::MemoryDB::SubnetGroup	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::NetworkFirewall::Firewall	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya	Ya
AWS::NetworkFirewall::FirewallPolicy	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya	Ya
AWS::NetworkFirewall::RuleGroup	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya	Ya
AWS::NetworkFirewall::TLSInspectionKonfigurasi	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya	Ya
AWS::NetworkFirewall::VpcEndpointAsosiasi	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya	Ya
AWS::OpenSearch::Domain	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::OpenSearchServerless::Collection	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::OpenSearchServerless::VpcEndpoint	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	Ya	Ya	Tidak	Tidak	Ya
AWS::Panorama::Package	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Tidak	Tidak	Tidak
AWS::Personalize::Dataset	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Personalize::DatasetGroup	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Personalize::Schema	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Personalize::Solution	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Pinpoint::App	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Pinpoint::ApplicationSettings	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Pinpoint::Campaign	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Pinpoint::EmailChannel	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::Pinpoint::EmailTemplate	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Pinpoint::EventStream	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Pinpoint::InAppTemplate	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Pinpoint::Segment	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::QLDB::Ledger	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::QuickSight::DataSource	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::QuickSight::Template	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::QuickSight::Theme	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS: :RDS::DBCluster	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS: :RDS::Snapshot DBCluster	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS: :RDS:: DBInstance	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS: :RDS:: Grup DBSecurity	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS: :RDS:: DBSnapshot	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS: :RDS:: Grup DBSubnet	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::RDS: :EventSubscription	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::RDS: :GlobalCluster	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::RDS: :OptionGroup	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::RUM: :AppMonitor	Tidak	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Redshift::Cluster	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Redshift::ClusterParameterKelompok	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::Redshift::ClusterSecurityKelompok	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Redshift::ClusterSnapshot	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Redshift::ClusterSubnetKelompok	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Redshift::EndpointAccess	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Redshift::EndpointAuthorization	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Redshift::EventSubscription	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::Redshift::ScheduledAction	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::ResilienceHub::App	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::ResilienceHub::ResiliencyPolicy	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::ResourceExplorer2::Index	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::RoboMaker::RobotApplication	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Ya
AWS::RoboMaker::RobotApplicationVersi	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Ya
AWS::RoboMaker::SimulationApplication	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Ya
AWS::Route53Profiles::Profile	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Route53Resolver::FirewallDomainDaftar	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Route53Resolver::FirewallRuleKelompok	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::Route53Resolver::FirewallRuleGroupAssociation	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Route53Resolver::ResolverEndpoint	Ya	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Route53Resolver::ResolverQueryLoggingConfig	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Route53Resolver::ResolverRule	Ya	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Route53Resolver::ResolverRuleAsosiasi	Ya	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::S3::AccessPoint	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::S3::AccountPublicAccessBlock	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::S3::Bucket	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::S3::StorageLens	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::S3::StorageLensKelompok	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::S3Express::BucketPolicy	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya
AWS::S3Express::DirectoryBucket	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya
AWS::SES::ConfigurationSet	Tidak	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::SES::ContactList	Tidak	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::SES::ReceiptFilter	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::SES::ReceiptRuleSet	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Tidak	Tidak	Ya
AWS::SES::Template	Tidak	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::SNS::Topic	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::SQS::Queue	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::SSM::AssociationCompliance	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Tidak	Ya	Ya
AWS::SSM::Document	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::SSM::FileData	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Tidak	Ya	Ya
AWS::SSM::ManagedInstanceInventaris	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya	Ya
AWS::SSM::PatchCompliance	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Tidak	Ya	Ya
AWS::SageMaker::AppImageConfig	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::SageMaker::CodeRepository	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::SageMaker::Domain	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::SageMaker::EndpointConfig	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::SageMaker::FeatureGroup	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::SageMaker::Image	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::SageMaker::InferenceExperiment	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::SageMaker::Model	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::SageMaker::NotebookInstance	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::SageMaker::NotebookInstanceLifecycleConfig	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::SageMaker::Workteam	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::SecretsManager::Secret	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya
AWS::SecurityHub::Standard	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya	Ya
AWS::ServiceCatalog::CloudFormationProduk	Ya	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Ya	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::ServiceCatalog::Portfolio	Ya	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::ServiceDiscovery::HttpNamespace	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::ServiceDiscovery::Instance	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::ServiceDiscovery::PublicDnsNamespace	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::ServiceDiscovery::Service	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::ShieldRegional::Protection	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Signer::SigningProfile	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::StepFunctions::Activity	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::StepFunctions::StateMachine	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Transfer::Agreement	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::Transfer::Certificate	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Transfer::Connector	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Transfer::Profile	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::Transfer::Workflow	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::WAFRegional::RateBasedAturan	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::WAFRegional::Rule	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::WAFRegional::RuleGroup	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::WAFRegional::WebACL	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::WAFv2:: IPSet	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya	Ya
AWS::WAFv2::ManagedRuleSet	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya	Ya

Jenis sumber daya	Asia Pasifik (Hong Kong)	Asia Pasifik (Hyderabad)	Asia Pasifik (Jakarta)	Asia Pasifik (Malaysia)	Asia Pasifik (Melbourne)	Asia Pasifik (Mumbai)	Asia Pasifik (Osaka)	Asia Pasifik (Seoul)	Asia Pasifik (Singapura)	Asia Pasifik (Sydney)	Asia Pasifik (Taipei)	Asia Pasifik (Thailand)	Asia Pasifik (Tokyo)
AWS::WAFv2::RegexPatternSet	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya	Ya
AWS::WAFv2::RuleGroup	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya	Ya
AWS::WAFv2::WebACL	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Ya	Ya
AWS::WorkSpaces::ConnectionAlias	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::WorkSpaces::Workspace	Tidak	Tidak	Tidak	Tidak	Tidak	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak	Ya
AWS::XRay::EncryptionConfig	Ya	Ya	Ya	Tidak	Ya	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya

Wilayah Tiongkok

Jenis sumber daya	Tiongkok (Beijing)	Tiongkok (Ningxia)
AWS::ACM::Certificate	Ya	Ya
AWS::AmazonMQ::Broker	Ya	Ya

Jenis sumber daya	Tiongkok (Beijing)	Tiongkok (Ningxia)
AWS::ApiGateway::RestApi	Ya	Ya
AWS::ApiGateway::Stage	Ya	Ya
AWS::ApiGatewayV2::Api	Ya	Ya
AWS::ApiGatewayV2::Stage	Ya	Ya
AWS::AppConfig::Application	Ya	Ya
AWS::AppConfig::ConfigurationProfile	Ya	Ya
AWS::AppConfig::DeploymentStrategy	Ya	Ya
AWS::AppConfig::Environment	Ya	Ya
AWS::AppConfig::ExtensionAssociation	Ya	Ya
AWS::AppConfig::HostedConfigurationVersi	Ya	Ya
AWS::AppSync::ApiCache	Ya	Ya
AWS::AppSync::GraphQLApi	Ya	Ya

Jenis sumber daya	Tiongkok (Beijing)	Tiongkok (Ningxia)
AWS::Athena::DataCatalog	Ya	Ya
AWS::Athena::PreparedStatement	Ya	Ya
AWS::Athena::WorkGroup	Ya	Ya
AWS::AutoScaling::AutoScalingKelompok	Ya	Ya
AWS::AutoScaling::LaunchConfiguration	Ya	Ya
AWS::AutoScaling::ScalingPolicy	Ya	Ya
AWS::AutoScaling::ScheduledAction	Ya	Ya
AWS::AutoScaling::WarmPool	Ya	Ya
AWS::Backup::BackupPlan	Ya	Ya
AWS::Backup::BackupSelection	Ya	Ya
AWS::Backup::BackupVault	Ya	Ya
AWS::Backup::RecoveryPoint	Ya	Ya

Jenis sumber daya	Tiongkok (Beijing)	Tiongkok (Ningxia)
AWS::Batch::ComputeEnvironment	Ya	Ya
AWS::Batch::JobQueue	Ya	Ya
AWS::Batch::SchedulingPolicy	Ya	Ya
AWS::Cassandra::Keyspace	Ya	Ya
AWS::CloudFormation::Stack	Ya	Ya
AWS::CloudTrail::Trail	Ya	Ya
AWS::CloudWatch::Alarm	Ya	Ya
AWS::CloudWatch::MetricStream	Ya	Ya
AWS::CodeBuild::Project	Ya	Ya
AWS::CodeBuild::ReportGroup	Ya	Ya
AWS::Cognito::IdentityPool	Ya	Tidak
AWS::Config::ConfigurationRecorder	Ya	Ya

Jenis sumber daya	Tiongkok (Beijing)	Tiongkok (Ningxia)
AWS::Config::ResourceCompliance	Ya	Ya
AWS::DMS::Certificate	Ya	Ya
AWS::DMS::Endpoint	Ya	Ya
AWS::DMS::EventSubscription	Ya	Ya
AWS::DMS::ReplicationInstance	Ya	Ya
AWS::DMS::ReplicationSubnetKelompok	Ya	Ya
AWS::DMS::ReplicationTask	Ya	Ya
AWS::DataSync::LocationEFS	Ya	Ya
AWS::DataSync::LocationHDFS	Ya	Ya
AWS::DataSync::LocationNFS	Ya	Ya
AWS::DataSync::LocationObjectPenyimpanan	Ya	Ya
AWS::DataSync::LocationS3	Ya	Ya

Jenis sumber daya	Tiongkok (Beijing)	Tiongkok (Ningxia)
AWS::DataSync::LocationSMB	Ya	Ya
AWS::DataSync::Task	Ya	Ya
AWS::DynamoDB::Table	Ya	Ya
AWS::EC2::CapacityReservation	Ya	Ya
AWS::EC2:: DHCPOptions	Ya	Ya
AWS:::EC2: EC2 Armada	Ya	Ya
AWS::EC2: :EIP	Ya	Ya
AWS::EC2:: EIPAssociation	Ya	Ya
AWS::EC2::FlowLog	Ya	Ya
AWS::EC2::Host	Ya	Ya
AWS::EC2::Instance	Ya	Ya
AWS::EC2::InternetGateway	Ya	Ya

Jenis sumber daya	Tiongkok (Beijing)	Tiongkok (Ningxia)
AWS::EC2::LaunchTemplate	Ya	Ya
AWS::EC2::NatGateway	Ya	Ya
AWS::EC2::NetworkAcl	Ya	Ya
AWS::EC2::NetworkInterface	Ya	Ya
AWS::EC2::PrefixList	Ya	Ya
AWS::EC2::RouteTable	Ya	Ya
AWS::EC2::SecurityGroup	Ya	Ya
AWS::EC2::SnapshotBlockPublicAccess	Ya	Ya
AWS::EC2::SpotFleet	Ya	Ya
AWS::EC2::Subnet	Ya	Ya
AWS::EC2::SubnetRouteTableAssociation	Ya	Ya
AWS::EC2::TrafficMirrorFilter	Ya	Ya

Jenis sumber daya	Tiongkok (Beijing)	Tiongkok (Ningxia)
AWS::EC2::TrafficMirrorSesi	Ya	Ya
AWS::EC2::TrafficMirrorTarget	Ya	Ya
AWS::EC2::TransitGateway	Ya	Ya
AWS::EC2::TransitGatewayLampiran	Ya	Ya
AWS::EC2::TransitGatewayConnect	Ya	Ya
AWS::EC2::TransitGatewayMulticastDomain	Ya	Ya
AWS::EC2::TransitGatewayRouteTable	Ya	Ya
AWS::EC2: :VPC	Ya	Ya
AWS::EC2:: VPCBlock PublicAccessExclusion	Ya	Ya
AWS::EC2:: VPCBlock PublicAccessOptions	Ya	Ya
AWS::EC2:: VPCEndpoint	Ya	Ya
AWS::EC2:: VPCEndpoint ConnectionNotification	Ya	Ya

Jenis sumber daya	Tiongkok (Beijing)	Tiongkok (Ningxia)
AWS::EC2:: VPCEndpoint Layanan	Ya	Ya
AWS::EC2:: VPCPeering Koneksi	Ya	Ya
AWS::EC2:: VPNGateway	Ya	Tidak
AWS::EC2::Volume	Ya	Ya
AWS::ECR::Repository	Ya	Ya
AWS::ECS::CapacityProvider	Ya	Ya
AWS::ECS::Cluster	Ya	Ya
AWS::ECS::Service	Ya	Ya
AWS::ECS::TaskDefinition	Ya	Ya
AWS::ECS::TaskSet	Ya	Ya
AWS::EFS::AccessPoint	Ya	Ya
AWS::EFS::FileSystem	Ya	Ya

Jenis sumber daya	Tiongkok (Beijing)	Tiongkok (Ningxia)
AWS::EKS::Addon	Ya	Ya
AWS::EKS::Cluster	Ya	Ya
AWS::EKS::FargateProfile	Ya	Ya
AWS::EKS::IdentityProviderConfig	Ya	Ya
AWS::EMR::SecurityConfiguration	Ya	Ya
AWS::ElasticBeanstalk::Application	Ya	Ya
AWS::ElasticBeanstalk::ApplicationVersion	Ya	Ya
AWS::ElasticBeanstalk::Environment	Ya	Ya
AWS::ElasticLoadBalancing::LoadBalancer	Ya	Ya
AWS::ElasticLoadBalancingV2::Listener	Ya	Ya
AWS::ElasticLoadBalancingV2::LoadBalancer	Ya	Ya
AWS::Elasticsearch::Domain	Ya	Ya

Jenis sumber daya	Tiongkok (Beijing)	Tiongkok (Ningxia)
AWS::Events::Archive	Ya	Ya
AWS::Events::EventBus	Ya	Ya
AWS::Events::Rule	Ya	Ya
AWS::Glue::Classifier	Ya	Ya
AWS::Glue::Job	Ya	Ya
AWS::Glue::MLTransform	Ya	Tidak
AWS::GreengrassV2::ComponentVersion	Ya	Tidak
AWS::GuardDuty::Filter	Ya	Ya
AWS::GuardDuty::ThreatIntelSet	Ya	Ya
AWS::IAM::Group	Ya	Ya
AWS::IAM::InstanceProfile	Ya	Tidak
AWS: :IAM:: OIDCProvider	Ya	Tidak

Jenis sumber daya	Tiongkok (Beijing)	Tiongkok (Ningxia)
AWS::IAM::Policy	Ya	Ya
AWS::IAM::Role	Ya	Ya
AWS: :IAM:: SAMLProvider	Ya	Tidak
AWS::IAM::ServerCertificate	Ya	Tidak
AWS::IAM::User	Ya	Ya
AWS::ImageBuilder::ContainerRecipe	Ya	Ya
AWS::ImageBuilder::DistributionConfiguration	Ya	Ya
AWS::ImageBuilder::ImagePipeline	Ya	Ya
AWS::ImageBuilder::ImageRecipe	Ya	Ya
AWS::ImageBuilder::InfrastructureConfiguration	Ya	Ya
AWS::InspectorV2::Activation	Ya	Ya
AWS::IoT::AccountAuditKonfigurasi	Ya	Ya

Jenis sumber daya	Tiongkok (Beijing)	Tiongkok (Ningxia)
AWS::IoT::Authorizer	Ya	Ya
AWS::IoT:: CACertificate	Ya	Ya
AWS::IoT::CustomMetric	Ya	Ya
AWS::IoT::Dimension	Ya	Ya
AWS::IoT::FleetMetric	Ya	Ya
AWS::IoT::JobTemplate	Ya	Ya
AWS::IoT::MitigationAction	Ya	Ya
AWS::IoT::Policy	Ya	Ya
AWS::IoT::ProvisioningTemplate	Ya	Ya
AWS::IoT::RoleAlias	Ya	Ya
AWS::IoT::ScheduledAudit	Ya	Ya
AWS::IoT::SecurityProfile	Ya	Ya

Jenis sumber daya	Tiongkok (Beijing)	Tiongkok (Ningxia)
AWS::IoTAnalytics::Channel	Ya	Tidak
AWS::IoTAnalytics::Dataset	Ya	Tidak
AWS::IoTAnalytics::Datastore	Ya	Tidak
AWS::IoTAnalytics::Pipeline	Ya	Tidak
AWS::IoTEvents::AlarmModel	Ya	Tidak
AWS::IoTEvents::DetectorModel	Ya	Tidak
AWS::IoTEvents::Input	Ya	Tidak
AWS::IoTSiteWise::AssetModel	Ya	Tidak
AWS::IoTSiteWise::Dashboard	Ya	Tidak
AWS::IoTSiteWise::Gateway	Ya	Tidak
AWS::IoTSiteWise::Portal	Ya	Tidak
AWS::IoTSiteWise::Project	Ya	Tidak

Jenis sumber daya	Tiongkok (Beijing)	Tiongkok (Ningxia)
AWS::KMS::Alias	Ya	Ya
AWS::KMS::Key	Ya	Ya
AWS::Kinesis::Stream	Ya	Ya
AWS::Kinesis::StreamConsumer	Ya	Ya
AWS::KinesisAnalyticsV2::Application	Ya	Ya
AWS::KinesisFirehose::DeliveryStream	Ya	Ya
AWS::Lambda::Function	Ya	Tidak
AWS::Logs::Destination	Ya	Ya
AWS::MSK::BatchScramRahasia	Ya	Ya
AWS::MSK::Cluster	Ya	Ya
AWS::MSK::ClusterPolicy	Ya	Ya
AWS::MSK::Configuration	Ya	Ya

Jenis sumber daya	Tiongkok (Beijing)	Tiongkok (Ningxia)
AWS::MSK::VpcConnection	Ya	Ya
AWS::NetworkFirewall::Firewall	Ya	Ya
AWS::NetworkFirewall::FirewallPolicy	Ya	Ya
AWS::NetworkFirewall::RuleGroup	Ya	Ya
AWS::NetworkFirewall:: TLSInspection Konfigurasi	Ya	Ya
AWS::NetworkFirewall::VpcEndpointAsosiasi	Ya	Ya
AWS::OpenSearch::Domain	Ya	Ya
AWS::Personalize::Dataset	Ya	Tidak
AWS::Personalize::DatasetGroup	Ya	Tidak
AWS::Personalize::Schema	Ya	Tidak
AWS::Personalize::Solution	Ya	Tidak
AWS: :RDS:: DBCluster	Tidak	Ya

Jenis sumber daya	Tiongkok (Beijing)	Tiongkok (Ningxia)
AWS: :RDS:: Snapshot DBCluster	Ya	Ya
AWS: :RDS:: DBInstance	Ya	Ya
AWS: :RDS:: Grup DBSecurity	Ya	Ya
AWS: :RDS:: DBSnapshot	Ya	Ya
AWS: :RDS:: Grup DBSubnet	Ya	Ya
AWS::RDS::EventSubscription	Ya	Ya
AWS::RDS::OptionGroup	Ya	Ya
AWS::Redshift::Cluster	Ya	Ya
AWS::Redshift::ClusterParameterKelompok	Ya	Ya
AWS::Redshift::ClusterSecurityKelompok	Ya	Ya
AWS::Redshift::ClusterSnapshot	Ya	Ya
AWS::Redshift::ClusterSubnetKelompok	Ya	Ya

Jenis sumber daya	Tiongkok (Beijing)	Tiongkok (Ningxia)
AWS::Redshift::EventSubscription	Ya	Ya
AWS::Route53Profiles::Profile	Ya	Ya
AWS::Route53Resolver::FirewallDomainDaftar	Ya	Ya
AWS::Route53Resolver::FirewallRuleGroupAssociation	Ya	Ya
AWS::Route53Resolver::ResolverEndpoint	Ya	Ya
AWS::Route53Resolver::ResolverQueryLoggingConfig	Ya	Ya
AWS::Route53Resolver::Resol verQueryLoggingConfigAssociation	Ya	Ya
AWS::Route53Resolver::ResolverRule	Ya	Ya
AWS::Route53Resolver::ResolverRuleAsosiasi	Ya	Ya
AWS::S3::AccessPoint	Ya	Ya
AWS::S3::AccountPublicAccessBlock	Ya	Ya
AWS::S3::Bucket	Ya	Ya

Jenis sumber daya	Tiongkok (Beijing)	Tiongkok (Ningxia)
AWS::S3::StorageLensKelompok	Ya	Ya
AWS::SES::ConfigurationSet	Tidak	Ya
AWS::SES::ContactList	Tidak	Ya
AWS::SES::Template	Tidak	Ya
AWS::SNS::Topic	Ya	Ya
AWS::SQS::Queue	Ya	Ya
AWS::SSM::AssociationCompliance	Ya	Ya
AWS::SSM::Document	Ya	Ya
AWS::SSM::FileData	Ya	Ya
AWS::SSM::ManagedInstanceInventaris	Ya	Ya
AWS::SSM::PatchCompliance	Ya	Ya
AWS::SageMaker::AppImageConfig	Ya	Ya

Jenis sumber daya	Tiongkok (Beijing)	Tiongkok (Ningxia)
AWS::SageMaker::CodeRepository	Ya	Ya
AWS::SageMaker::Domain	Ya	Ya
AWS::SageMaker::EndpointConfig	Ya	Ya
AWS::SageMaker::FeatureGroup	Ya	Ya
AWS::SageMaker::Image	Ya	Ya
AWS::SageMaker::Model	Ya	Ya
AWS::SageMaker::NotebookInstance	Ya	Ya
AWS::SageMaker::NotebookInstanceLifecycleConfig	Ya	Ya
AWS::SecretsManager::Secret	Ya	Ya
AWS::SecurityHub::Standard	Ya	Ya
AWS::ServiceCatalog::CloudFormationProduk	Ya	Ya
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Ya	Ya

Jenis sumber daya	Tiongkok (Beijing)	Tiongkok (Ningxia)
AWS::ServiceCatalog::Portfolio	Ya	Ya
AWS::ServiceDiscovery::HttpNamespace	Ya	Ya
AWS::ServiceDiscovery::Instance	Ya	Ya
AWS::ServiceDiscovery::PublicDnsNamespace	Ya	Ya
AWS::ServiceDiscovery::Service	Ya	Ya
AWS::StepFunctions::Activity	Ya	Tidak
AWS::StepFunctions::StateMachine	Ya	Ya
AWS::Transfer::Agreement	Ya	Ya
AWS::Transfer::Certificate	Ya	Ya
AWS::Transfer::Connector	Ya	Ya
AWS::Transfer::Profile	Ya	Ya
AWS::Transfer::Workflow	Ya	Ya

Jenis sumber daya	Tiongkok (Beijing)	Tiongkok (Ningxia)
AWS::WAFRegional::RateBasedAturan	Ya	Ya
AWS::WAFRegional::Rule	Ya	Ya
AWS::WAFRegional::RuleGroup	Ya	Ya
AWS::WAFRegional::WebACL	Ya	Ya
AWS::WAFv2:: IPSet	Ya	Ya
AWS::WAFv2::ManagedRuleSet	Ya	Ya
AWS::WAFv2::RegexPatternSet	Ya	Ya
AWS::WAFv2::RuleGroup	Ya	Ya
AWS::WAFv2::WebACL	Ya	Ya
AWS::WorkSpaces::Workspace	Tidak	Ya

Wilayah Afrika dan Timur Tengah

Jenis sumber daya	Afrika (Cape Town)	Israel (Tel Aviv)	Timur Tengah (Bahrain)	Timur Tengah (UEA)
AWS::ACM::Certificate	Ya	Ya	Ya	Ya
AWS::ACMPCA::CertificateAuthority	Ya	Ya	Ya	Ya
AWS::ACMPCA::CertificateAuthorityAktivasi	Ya	Ya	Ya	Ya
AWS::AccessAnalyzer::Analyzer	Ya	Ya	Ya	Ya
AWS::AmazonMQ::Broker	Ya	Tidak	Ya	Ya
AWS::Amplify::App	Tidak	Tidak	Ya	Tidak
AWS::Amplify::Branch	Tidak	Tidak	Ya	Tidak
AWS::ApiGateway::RestApi	Ya	Ya	Ya	Ya
AWS::ApiGateway::Stage	Ya	Ya	Ya	Ya
AWS::ApiGatewayV2::Api	Ya	Ya	Ya	Ya
AWS::ApiGatewayV2::Stage	Ya	Ya	Ya	Ya

Jenis sumber daya	Afrika (Cape Town)	Israel (Tel Aviv)	Timur Tengah (Bahrain)	Timur Tengah (UEA)
AWS::AppConfig::Application	Ya	Ya	Ya	Tidak
AWS::AppConfig::ConfigurationProfile	Ya	Ya	Ya	Tidak
AWS::AppConfig::DeploymentStrategy	Ya	Ya	Ya	Ya
AWS::AppConfig::Environment	Ya	Ya	Ya	Tidak
AWS::AppConfig::ExtensionAssociation	Ya	Ya	Ya	Ya
AWS::AppConfig::HostedConfigurationVersi	Ya	Ya	Ya	Tidak
AWS::AppFlow::Flow	Ya	Tidak	Tidak	Tidak
AWS::AppIntegrations::Application	Ya	Tidak	Tidak	Tidak
AWS::AppIntegrations::EventIntegration	Ya	Tidak	Tidak	Tidak
AWS::AppMesh::GatewayRoute	Ya	Ya	Ya	Tidak
AWS::AppMesh::Mesh	Ya	Ya	Ya	Tidak
AWS::AppMesh::Route	Ya	Ya	Ya	Tidak

Jenis sumber daya	Afrika (Cape Town)	Israel (Tel Aviv)	Timur Tengah (Bahrain)	Timur Tengah (UEA)
AWS::AppMesh::VirtualGateway	Ya	Ya	Ya	Tidak
AWS::AppMesh::VirtualNode	Ya	Ya	Ya	Tidak
AWS::AppMesh::VirtualRouter	Ya	Ya	Ya	Tidak
AWS::AppMesh::VirtualService	Ya	Ya	Ya	Tidak
AWS::AppSync::ApiCache	Ya	Ya	Ya	Ya
AWS::AppSync::GraphQLApi	Ya	Ya	Ya	Ya
AWS::Athena::DataCatalog	Ya	Ya	Ya	Ya
AWS::Athena::PreparedStatement	Ya	Ya	Ya	Ya
AWS::Athena::WorkGroup	Ya	Ya	Ya	Ya
AWS::AutoScaling::AutoScalingKelompok	Ya	Ya	Ya	Ya
AWS::AutoScaling::LaunchConfiguration	Ya	Ya	Ya	Ya
AWS::AutoScaling::ScalingPolicy	Ya	Ya	Ya	Ya

Jenis sumber daya	Afrika (Cape Town)	Israel (Tel Aviv)	Timur Tengah (Bahrain)	Timur Tengah (UEA)
AWS::AutoScaling::ScheduledAction	Ya	Ya	Ya	Ya
AWS::AutoScaling::WarmPool	Ya	Tidak	Ya	Tidak
AWS::Backup::BackupPlan	Ya	Ya	Ya	Ya
AWS::Backup::BackupSelection	Ya	Ya	Ya	Ya
AWS::Backup::BackupVault	Ya	Ya	Ya	Ya
AWS::Backup::RecoveryPoint	Ya	Ya	Ya	Ya
AWS::Backup::ReportPlan	Ya	Tidak	Ya	Tidak
AWS::Batch::ComputeEnvironment	Ya	Tidak	Ya	Ya
AWS::Batch::JobQueue	Ya	Tidak	Ya	Ya
AWS::Batch::SchedulingPolicy	Ya	Ya	Ya	Ya
AWS::Cassandra::Keyspace	Tidak	Tidak	Ya	Tidak
AWS::Cloud9::EnvironmentEC2	Ya	Tidak	Ya	Tidak

Jenis sumber daya	Afrika (Cape Town)	Israel (Tel Aviv)	Timur Tengah (Bahrain)	Timur Tengah (UEA)
AWS::CloudFormation::Stack	Ya	Tidak	Ya	Tidak
AWS::CloudTrail::Trail	Ya	Ya	Ya	Ya
AWS::CloudWatch::Alarm	Ya	Ya	Ya	Ya
AWS::CloudWatch::MetricStream	Ya	Ya	Ya	Ya
AWS::CodeBuild::Project	Ya	Ya	Ya	Ya
AWS::CodeBuild::ReportGroup	Ya	Ya	Ya	Ya
AWS::CodeDeploy::Application	Ya	Tidak	Ya	Tidak
AWS::CodeDeploy::DeploymentConfig	Ya	Tidak	Ya	Tidak
AWS::CodeDeploy::DeploymentGroup	Ya	Tidak	Ya	Tidak
AWS::CodePipeline::Pipeline	Tidak	Ya	Tidak	Ya
AWS::Cognito::IdentityPool	Ya	Ya	Ya	Ya
AWS::Cognito::UserPool	Ya	Ya	Ya	Ya

Jenis sumber daya	Afrika (Cape Town)	Israel (Tel Aviv)	Timur Tengah (Bahrain)	Timur Tengah (UEA)
AWS::Cognito::UserPoolKlien	Ya	Ya	Ya	Ya
AWS::Cognito::UserPoolKelompok	Ya	Ya	Ya	Ya
AWS::Config::ConfigurationRecorder	Ya	Ya	Ya	Ya
AWS::Config::ConformancePackKepatuhan	Ya	Ya	Ya	Ya
AWS::Config::ResourceCompliance	Ya	Ya	Ya	Ya
AWS::Connect::Instance	Ya	Tidak	Tidak	Tidak
AWS::Connect::PhoneNumber	Ya	Tidak	Tidak	Tidak
AWS::Connect::QuickConnect	Ya	Tidak	Tidak	Tidak
AWS::Connect::Rule	Ya	Tidak	Tidak	Tidak
AWS::Connect::User	Ya	Tidak	Tidak	Tidak
AWS::CustomerProfiles::Domain	Ya	Tidak	Tidak	Tidak
AWS::CustomerProfiles::ObjectType	Ya	Tidak	Tidak	Tidak

Jenis sumber daya	Afrika (Cape Town)	Israel (Tel Aviv)	Timur Tengah (Bahrain)	Timur Tengah (UEA)
AWS::DMS::Certificate	Ya	Tidak	Ya	Tidak
AWS::DMS::Endpoint	Ya	Tidak	Ya	Tidak
AWS::DMS::EventSubscription	Ya	Tidak	Ya	Tidak
AWS::DMS::ReplicationInstance	Ya	Tidak	Ya	Tidak
AWS::DMS::ReplicationSubnetKelompok	Ya	Tidak	Ya	Tidak
AWS::DMS::ReplicationTask	Ya	Tidak	Ya	Tidak
AWS::DataSync::LocationEFS	Ya	Tidak	Ya	Ya
AWS::DataSync::LocationFSxKilau	Ya	Tidak	Ya	Tidak
AWS::DataSync::LocationFSxJendela	Ya	Tidak	Ya	Tidak
AWS::DataSync::LocationHDFS	Ya	Tidak	Ya	Ya
AWS::DataSync::LocationNFS	Ya	Tidak	Ya	Ya
AWS::DataSync::LocationObjectPenyimpanan	Ya	Tidak	Ya	Ya

Jenis sumber daya	Afrika (Cape Town)	Israel (Tel Aviv)	Timur Tengah (Bahrain)	Timur Tengah (UEA)
AWS::DataSync::LocationS3	Ya	Ya	Ya	Ya
AWS::DataSync::LocationSMB	Ya	Tidak	Ya	Ya
AWS::DataSync::Task	Ya	Ya	Ya	Ya
AWS::Detective::Graph	Ya	Ya	Ya	Tidak
AWS::DynamoDB::Table	Ya	Ya	Ya	Ya
AWS::EC2::CapacityReservation	Ya	Ya	Ya	Ya
AWS::EC2::ClientVpnTitik akhir	Ya	Tidak	Ya	Tidak
AWS::EC2::ClientVpnTargetNetworkAssociation	Ya	Ya	Ya	Tidak
AWS::EC2::CustomerGateway	Ya	Ya	Ya	Ya
AWS::EC2:: DHCPOptions	Ya	Ya	Ya	Ya
AWS:::EC2: EC2 Armada	Ya	Tidak	Ya	Ya
AWS::EC2: :EIP	Ya	Ya	Ya	Ya

Jenis sumber daya	Afrika (Cape Town)	Israel (Tel Aviv)	Timur Tengah (Bahrain)	Timur Tengah (UEA)
AWS::EC2:: EIPAssociation	Ya	Ya	Ya	Ya
AWS::EC2::EgressOnlyInternetGateway	Ya	Tidak	Ya	Ya
AWS::EC2::FlowLog	Ya	Tidak	Ya	Ya
AWS::EC2::Host	Ya	Ya	Ya	Ya
AWS::EC2: :IPAM	Ya	Tidak	Ya	Ya
AWS::EC2:: IPAMPool	Ya	Tidak	Ya	Ya
AWS::EC2:: IPAMResource Penemuan	Ya	Ya	Ya	Ya
AWS::EC2:: IPAMResou rce DiscoveryAssociation	Ya	Ya	Ya	Ya
AWS::EC2:: IPAMScope	Ya	Tidak	Ya	Ya
AWS::EC2::Instance	Ya	Ya	Ya	Ya
AWS::EC2::InstanceConnectTitik akhir	Ya	Ya	Ya	Ya
AWS::EC2::InternetGateway	Ya	Ya	Ya	Ya

Jenis sumber daya	Afrika (Cape Town)	Israel (Tel Aviv)	Timur Tengah (Bahrain)	Timur Tengah (UEA)
AWS::EC2::LaunchTemplate	Ya	Tidak	Ya	Tidak
AWS::EC2::NatGateway	Ya	Tidak	Ya	Ya
AWS::EC2::NetworkAcl	Ya	Ya	Ya	Ya
AWS::EC2::NetworkInsightsAccessScope	Ya	Tidak	Ya	Tidak
AWS::EC2::NetworkI nsightsAccessScopeAnalysis	Ya	Tidak	Ya	Tidak
AWS::EC2::NetworkInsightsAnalisa	Ya	Tidak	Ya	Tidak
AWS::EC2::NetworkInsightsJalan	Ya	Tidak	Ya	Tidak
AWS::EC2::NetworkInterface	Ya	Ya	Ya	Ya
AWS::EC2::PrefixList	Ya	Ya	Ya	Ya
AWS::EC2::RouteTable	Ya	Ya	Ya	Ya
AWS::EC2::SecurityGroup	Ya	Ya	Ya	Ya
AWS::EC2::SnapshotBlockPublicAccess	Ya	Ya	Ya	Ya

Jenis sumber daya	Afrika (Cape Town)	Israel (Tel Aviv)	Timur Tengah (Bahrain)	Timur Tengah (UEA)
AWS::EC2::SpotFleet	Ya	Ya	Ya	Ya
AWS::EC2::Subnet	Ya	Ya	Ya	Ya
AWS::EC2::SubnetRouteTableAssociation	Ya	Ya	Ya	Ya
AWS::EC2::TrafficMirrorFilter	Ya	Ya	Ya	Ya
AWS::EC2::TrafficMirrorSesi	Tidak	Tidak	Ya	Tidak
AWS::EC2::TrafficMirrorTarget	Tidak	Tidak	Ya	Tidak
AWS::EC2::TransitGateway	Ya	Ya	Ya	Ya
AWS::EC2::TransitGatewayLampiran	Ya	Tidak	Ya	Ya
AWS::EC2::TransitGatewayConnect	Ya	Tidak	Ya	Ya
AWS::EC2::TransitG atewayMulticastDomain	Ya	Ya	Ya	Ya
AWS::EC2::TransitGatewayRouteTable	Ya	Tidak	Ya	Ya
AWS::EC2: :VPC	Ya	Ya	Ya	Ya

Jenis sumber daya	Afrika (Cape Town)	Israel (Tel Aviv)	Timur Tengah (Bahrain)	Timur Tengah (UEA)
AWS::EC2:: VPCBlock PublicAccessExclusion	Ya	Ya	Ya	Ya
AWS::EC2:: VPCBlock PublicAccessOptions	Ya	Ya	Ya	Ya
AWS::EC2:: VPCEndpoint	Ya	Ya	Ya	Ya
AWS::EC2:: VPCEndpoi nt ConnectionNotification	Ya	Ya	Ya	Ya
AWS::EC2:: VPCEndpoint Layanan	Ya	Ya	Ya	Ya
AWS::EC2:: VPCPeering Koneksi	Ya	Ya	Ya	Ya
AWS::EC2:: VPNConnection	Ya	Ya	Ya	Ya
AWS::EC2:: VPNConnection Rute	Ya	Ya	Ya	Ya
AWS::EC2:: VPNGateway	Ya	Ya	Ya	Ya
AWS::EC2::Volume	Ya	Ya	Ya	Ya
AWS::ECR::PullThroughCacheRule	Ya	Ya	Ya	Ya
AWS::ECR::RegistryPolicy	Ya	Ya	Ya	Ya

Jenis sumber daya	Afrika (Cape Town)	Israel (Tel Aviv)	Timur Tengah (Bahrain)	Timur Tengah (UEA)
AWS::ECR::Repository	Ya	Ya	Ya	Ya
AWS::ECS::CapacityProvider	Ya	Ya	Ya	Ya
AWS::ECS::Cluster	Ya	Ya	Ya	Ya
AWS::ECS::Service	Ya	Ya	Ya	Ya
AWS::ECS::TaskDefinition	Ya	Ya	Ya	Ya
AWS::ECS::TaskSet	Ya	Tidak	Ya	Ya
AWS::EFS::AccessPoint	Ya	Ya	Ya	Ya
AWS::EFS::FileSystem	Ya	Ya	Ya	Ya
AWS::EKS::Addon	Ya	Tidak	Ya	Ya
AWS::EKS::Cluster	Ya	Tidak	Ya	Ya
AWS::EKS::FargateProfile	Ya	Ya	Ya	Ya
AWS::EKS::IdentityProviderConfig	Ya	Tidak	Ya	Ya

Jenis sumber daya	Afrika (Cape Town)	Israel (Tel Aviv)	Timur Tengah (Bahrain)	Timur Tengah (UEA)
AWS::EMR::SecurityConfiguration	Ya	Ya	Ya	Ya
AWS::ElasticBeanstalk::Application	Ya	Tidak	Ya	Ya
AWS::ElasticBeanstalk::ApplicationVersion	Ya	Tidak	Ya	Ya
AWS::ElasticBeanstalk::Environment	Ya	Tidak	Ya	Ya
AWS::ElasticLoadBalancing::LoadBalancer	Ya	Ya	Ya	Ya
AWS::ElasticLoadBalancingV2::Listener	Ya	Tidak	Ya	Tidak
AWS::ElasticLoadBalancingV2::LoadBalancer	Ya	Ya	Ya	Ya
AWS::Elasticsearch::Domain	Ya	Ya	Ya	Ya
AWS::EventSchemas::Discoverer	Ya	Tidak	Ya	Ya
AWS::EventSchemas::Registry	Ya	Tidak	Ya	Ya
AWS::EventSchemas::RegistryPolicy	Ya	Tidak	Ya	Ya
AWS::EventSchemas::Schema	Ya	Tidak	Ya	Ya

Jenis sumber daya	Afrika (Cape Town)	Israel (Tel Aviv)	Timur Tengah (Bahrain)	Timur Tengah (UEA)
AWS::Events::ApiDestination	Ya	Tidak	Ya	Ya
AWS::Events::Archive	Ya	Tidak	Ya	Ya
AWS::Events::Connection	Ya	Tidak	Ya	Ya
AWS::Events::EventBus	Ya	Ya	Ya	Ya
AWS::Events::Rule	Ya	Tidak	Ya	Tidak
AWS::FIS::ExperimentTemplate	Ya	Tidak	Ya	Tidak
AWS::Glue::Classifier	Ya	Ya	Ya	Ya
AWS::Glue::Job	Ya	Ya	Ya	Ya
AWS::Glue::MLTransform	Ya	Ya	Ya	Ya
AWS::GroundStation::Config	Ya	Tidak	Ya	Tidak
AWS::GroundStation ::DataflowEndpointKelompok	Ya	Tidak	Ya	Tidak
AWS::GroundStation::MissionProfile	Ya	Tidak	Ya	Tidak

Jenis sumber daya	Afrika (Cape Town)	Israel (Tel Aviv)	Timur Tengah (Bahrain)	Timur Tengah (UEA)
AWS::GuardDuty::Detector	Ya	Ya	Ya	Ya
AWS::GuardDuty::Filter	Ya	Tidak	Ya	Tidak
AWS::GuardTugas:: IPSet	Ya	Tidak	Ya	Ya
AWS::GuardDuty::ThreatIntelSet	Ya	Ya	Ya	Ya
AWS::IAM::Group	Ya	Tidak	Ya	Tidak
AWS::IAM::Policy	Ya	Tidak	Ya	Tidak
AWS::IAM::Role	Ya	Tidak	Ya	Tidak
AWS::IAM::User	Ya	Tidak	Ya	Tidak
AWS::ImageBuilder::ContainerRecipe	Ya	Ya	Ya	Ya
AWS::ImageBuilder: :DistributionConfiguration	Ya	Ya	Ya	Ya
AWS::ImageBuilder::ImagePipeline	Ya	Ya	Ya	Ya
AWS::ImageBuilder::ImageRecipe	Ya	Ya	Ya	Ya

Jenis sumber daya	Afrika (Cape Town)	Israel (Tel Aviv)	Timur Tengah (Bahrain)	Timur Tengah (UEA)
AWS::ImageBuilder::InfrastructureConfiguration	Ya	Ya	Ya	Ya
AWS::InspectorV2::Activation	Ya	Tidak	Ya	Tidak
AWS::InspectorV2::Filter	Ya	Tidak	Ya	Tidak
AWS::IoT::AccountAuditKonfigurasi	Tidak	Tidak	Ya	Ya
AWS::IoT::Authorizer	Tidak	Tidak	Ya	Ya
AWS::IoT:: CACertificate	Tidak	Tidak	Ya	Ya
AWS::IoT::CustomMetric	Tidak	Tidak	Ya	Ya
AWS::IoT::Dimension	Tidak	Tidak	Ya	Ya
AWS::IoT::FleetMetric	Tidak	Tidak	Ya	Ya
AWS::IoT::JobTemplate	Tidak	Tidak	Ya	Ya
AWS::IoT::MitigationAction	Tidak	Tidak	Ya	Ya
AWS::IoT::Policy	Tidak	Tidak	Ya	Ya

Jenis sumber daya	Afrika (Cape Town)	Israel (Tel Aviv)	Timur Tengah (Bahrain)	Timur Tengah (UEA)
AWS::IoT::ProvisioningTemplate	Tidak	Tidak	Ya	Ya
AWS::IoT::RoleAlias	Tidak	Tidak	Ya	Ya
AWS::IoT::ScheduledAudit	Tidak	Tidak	Ya	Ya
AWS::IoT::SecurityProfile	Tidak	Tidak	Ya	Ya
AWS::KMS::Alias	Ya	Tidak	Ya	Ya
AWS::KMS::Key	Ya	Ya	Ya	Ya
AWS::Kinesis::Stream	Ya	Tidak	Ya	Ya
AWS::Kinesis::StreamConsumer	Ya	Ya	Ya	Ya
AWS::KinesisAnalyticsV2::Application	Ya	Ya	Ya	Ya
AWS::KinesisFirehose::DeliveryStream	Ya	Ya	Ya	Ya
AWS::Lambda::CodeSigningConfig	Ya	Tidak	Ya	Tidak
AWS::Lambda::Function	Ya	Ya	Ya	Ya

Jenis sumber daya	Afrika (Cape Town)	Israel (Tel Aviv)	Timur Tengah (Bahrain)	Timur Tengah (UEA)
AWS::Lex::Bot	Ya	Tidak	Tidak	Tidak
AWS::Lex::BotAlias	Ya	Tidak	Tidak	Tidak
AWS::Logs::Destination	Ya	Ya	Ya	Ya
AWS::MSK::BatchScramRahasia	Ya	Tidak	Ya	Ya
AWS::MSK::Cluster	Ya	Tidak	Ya	Ya
AWS::MSK::ClusterPolicy	Ya	Ya	Ya	Ya
AWS::MSK::Configuration	Ya	Ya	Ya	Ya
AWS::MSK::VpcConnection	Ya	Ya	Ya	Ya
AWS::Macie::Session	Ya	Ya	Ya	Tidak
AWS::MediaConnect::FlowEntitlement	Ya	Tidak	Tidak	Ya
AWS::MediaConnect::FlowSource	Ya	Tidak	Tidak	Ya
AWS::MediaConnect::FlowVpcAntarmuka	Ya	Tidak	Tidak	Tidak

Jenis sumber daya	Afrika (Cape Town)	Israel (Tel Aviv)	Timur Tengah (Bahrain)	Timur Tengah (UEA)
AWS::MediaConnect::Gateway	Ya	Tidak	Tidak	Tidak
AWS::MediaTailor::PlaybackConfiguration	Ya	Tidak	Tidak	Ya
AWS::NetworkFirewall::Firewall	Ya	Ya	Ya	Ya
AWS::NetworkFirewall::FirewallPolicy	Ya	Ya	Ya	Ya
AWS::NetworkFirewall::RuleGroup	Ya	Ya	Ya	Ya
AWS::NetworkFirewall:: TLSInspection Konfigurasi	Ya	Ya	Ya	Ya
AWS::NetworkFirewa ll::VpcEndpointAsosiasi	Ya	Ya	Ya	Ya
AWS::OpenSearch::Domain	Ya	Tidak	Ya	Tidak
AWS: :RDS:: DBCluster	Ya	Ya	Ya	Ya
AWS: :RDS:: Snapshot DBCluster	Ya	Tidak	Ya	Ya
AWS: :RDS:: DBInstance	Ya	Ya	Ya	Ya
AWS: :RDS:: Grup DBSecurity	Ya	Ya	Ya	Ya

Jenis sumber daya	Afrika (Cape Town)	Israel (Tel Aviv)	Timur Tengah (Bahrain)	Timur Tengah (UEA)
AWS: :RDS:: DBSnapshot	Ya	Ya	Ya	Ya
AWS: :RDS:: Grup DBSubnet	Ya	Ya	Ya	Ya
AWS::RDS::EventSubscription	Ya	Ya	Ya	Ya
AWS::RDS::GlobalCluster	Ya	Ya	Ya	Ya
AWS::RDS::OptionGroup	Ya	Ya	Ya	Ya
AWS::RUM::AppMonitor	Tidak	Tidak	Ya	Ya
AWS::Redshift::Cluster	Ya	Ya	Ya	Ya
AWS::Redshift::ClusterParameterKelompok	Ya	Ya	Ya	Ya
AWS::Redshift::ClusterSecurityKelompok	Ya	Ya	Ya	Ya
AWS::Redshift::ClusterSnapshot	Ya	Ya	Ya	Ya
AWS::Redshift::ClusterSubnetKelompok	Ya	Ya	Ya	Ya
AWS::Redshift::EventSubscription	Ya	Ya	Ya	Ya

Jenis sumber daya	Afrika (Cape Town)	Israel (Tel Aviv)	Timur Tengah (Bahrain)	Timur Tengah (UEA)
AWS::Redshift::ScheduledAction	Tidak	Tidak	Ya	Tidak
AWS::ResilienceHub::App	Ya	Tidak	Ya	Tidak
AWS::ResilienceHub::ResiliencyPolicy	Ya	Tidak	Ya	Tidak
AWS::ResourceExplorer2::Index	Tidak	Tidak	Ya	Ya
AWS::Route53Profiles::Profile	Ya	Ya	Ya	Ya
AWS::Route53Resolver::FirewallDomainDaftar	Ya	Tidak	Ya	Tidak
AWS::Route53Resolver::FirewallRuleKelompok	Ya	Tidak	Ya	Tidak
AWS::Route53Resolver::FirewallRuleGroupAssociation	Ya	Tidak	Ya	Tidak
AWS::Route53Resolver::ResolverEndpoint	Ya	Tidak	Ya	Ya
AWS::Route53Resolver::ResolverQueryLoggingConfig	Ya	Tidak	Ya	Tidak
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	Ya	Tidak	Ya	Tidak
AWS::Route53Resolver::ResolverRule	Ya	Tidak	Ya	Ya

Jenis sumber daya	Afrika (Cape Town)	Israel (Tel Aviv)	Timur Tengah (Bahrain)	Timur Tengah (UEA)
AWS::Route53Resolver::ResolverRuleAsosiasi	Ya	Tidak	Ya	Ya
AWS::S3::AccessPoint	Ya	Ya	Ya	Ya
AWS::S3::AccountPublicAccessBlock	Ya	Tidak	Ya	Ya
AWS::S3::Bucket	Ya	Ya	Ya	Ya
AWS::SES::ConfigurationSet	Ya	Ya	Ya	Tidak
AWS::SES::ContactList	Ya	Ya	Ya	Tidak
AWS::SES::Template	Ya	Ya	Ya	Tidak
AWS::SNS::Topic	Ya	Ya	Ya	Ya
AWS::SQS::Queue	Ya	Tidak	Ya	Tidak
AWS::SSM::AssociationCompliance	Ya	Ya	Ya	Ya
AWS::SSM::Document	Ya	Ya	Ya	Ya
AWS::SSM::FileData	Ya	Ya	Ya	Ya

Jenis sumber daya	Afrika (Cape Town)	Israel (Tel Aviv)	Timur Tengah (Bahrain)	Timur Tengah (UEA)
AWS::SSM::ManagedInstanceInventaris	Ya	Ya	Ya	Ya
AWS::SSM::PatchCompliance	Ya	Ya	Ya	Ya
AWS::SageMaker::AppImageConfig	Ya	Ya	Ya	Ya
AWS::SageMaker::CodeRepository	Ya	Tidak	Ya	Tidak
AWS::SageMaker::Domain	Ya	Tidak	Ya	Tidak
AWS::SageMaker::EndpointConfig	Ya	Tidak	Ya	Tidak
AWS::SageMaker::FeatureGroup	Ya	Ya	Ya	Tidak
AWS::SageMaker::Image	Ya	Ya	Ya	Ya
AWS::SageMaker::InferenceExperiment	Ya	Tidak	Ya	Tidak
AWS::SageMaker::Model	Ya	Tidak	Ya	Tidak
AWS::SageMaker::NotebookInstance	Ya	Tidak	Ya	Tidak
AWS::SageMaker::NotebookInstanceLifecycleConfig	Ya	Tidak	Ya	Tidak

Jenis sumber daya	Afrika (Cape Town)	Israel (Tel Aviv)	Timur Tengah (Bahrain)	Timur Tengah (UEA)
AWS::SecretsManager::Secret	Ya	Ya	Ya	Ya
AWS::SecurityHub::Standard	Ya	Ya	Ya	Ya
AWS::ServiceCatalog::CloudFormationProduk	Ya	Tidak	Ya	Ya
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Ya	Tidak	Ya	Ya
AWS::ServiceCatalog::Portfolio	Ya	Tidak	Ya	Ya
AWS::ServiceDiscovery::HttpNamespace	Ya	Ya	Ya	Ya
AWS::ServiceDiscovery::Instance	Ya	Tidak	Ya	Ya
AWS::ServiceDiscovery::PublicDnsNamespace	Ya	Ya	Ya	Ya
AWS::ServiceDiscovery::Service	Ya	Tidak	Ya	Ya
AWS::ShieldRegional::Protection	Ya	Tidak	Ya	Ya
AWS::Signer::SigningProfile	Ya	Tidak	Ya	Tidak
AWS::StepFunctions::Activity	Ya	Ya	Ya	Ya

Jenis sumber daya	Afrika (Cape Town)	Israel (Tel Aviv)	Timur Tengah (Bahrain)	Timur Tengah (UEA)
AWS::StepFunctions::StateMachine	Ya	Ya	Ya	Ya
AWS::Transfer::Agreement	Ya	Tidak	Ya	Ya
AWS::Transfer::Certificate	Ya	Ya	Ya	Ya
AWS::Transfer::Connector	Ya	Ya	Ya	Ya
AWS::Transfer::Profile	Ya	Ya	Ya	Ya
AWS::Transfer::Workflow	Ya	Ya	Ya	Ya
AWS::WAFRegional::RateBasedAturan	Ya	Ya	Ya	Ya
AWS::WAFRegional::Rule	Ya	Ya	Ya	Ya
AWS::WAFRegional::RuleGroup	Ya	Ya	Ya	Ya
AWS::WAFRegional::WebACL	Ya	Ya	Ya	Ya
AWS::WAFv2:: IPSet	Ya	Ya	Ya	Ya
AWS::WAFv2::ManagedRuleSet	Ya	Ya	Ya	Ya

Jenis sumber daya	Afrika (Cape Town)	Israel (Tel Aviv)	Timur Tengah (Bahrain)	Timur Tengah (UEA)
AWS::WAFv2::RegexPatternSet	Ya	Ya	Ya	Ya
AWS::WAFv2::RuleGroup	Ya	Ya	Ya	Ya
AWS::WAFv2::WebACL	Ya	Ya	Ya	Ya
AWS::WorkSpaces::Workspace	Ya	Tidak	Tidak	Tidak
AWS::XRay::EncryptionConfig	Ya	Ya	Tidak	Ya

GovCloud Daerah

Jenis sumber daya	AWS GovCloud (AS-Barat)	AWS GovCloud (AS-Timur)
AWS::ACM::Certificate	Ya	Ya
AWS::ACMPCA::CertificateAuthority	Ya	Ya
AWS::ACMPCA::CertificateAuthorityAktivasi	Ya	Ya
AWS::AccessAnalyzer::Analyzer	Ya	Ya

Jenis sumber daya	AWS GovCloud (AS-Barat)	AWS GovCloud (AS-Timur)
AWS::AmazonMQ::Broker	Ya	Ya
AWS::ApiGateway::RestApi	Ya	Ya
AWS::ApiGateway::Stage	Ya	Ya
AWS::ApiGatewayV2::Api	Ya	Ya
AWS::ApiGatewayV2::Stage	Ya	Ya
AWS::AppConfig::Application	Ya	Ya
AWS::AppConfig::ConfigurationProfile	Ya	Ya
AWS::AppConfig::DeploymentStrategy	Ya	Ya
AWS::AppConfig::Environment	Ya	Ya
AWS::AppConfig::ExtensionAssociation	Ya	Ya
AWS::AppConfig::HostedConfigurationVersi	Ya	Ya
AWS::AppStream::Application	Ya	Ya

Jenis sumber daya	AWS GovCloud (AS-Barat)	AWS GovCloud (AS-Timur)
AWS::AppStream::DirectoryConfig	Ya	Tidak
AWS::AppStream::Fleet	Ya	Tidak
AWS::AppStream::Stack	Ya	Tidak
AWS::Athena::DataCatalog	Ya	Ya
AWS::Athena::WorkGroup	Ya	Ya
AWS::AutoScaling::AutoScalingKelompok	Ya	Ya
AWS::AutoScaling::LaunchConfiguration	Ya	Ya
AWS::AutoScaling::ScalingPolicy	Ya	Ya
AWS::AutoScaling::ScheduledAction	Ya	Ya
AWS::AutoScaling::WarmPool	Ya	Ya
AWS::Backup::BackupPlan	Ya	Ya
AWS::Backup::BackupSelection	Ya	Ya

Jenis sumber daya	AWS GovCloud (AS-Barat)	AWS GovCloud (AS-Timur)
AWS::Backup::BackupVault	Ya	Ya
AWS::Backup::RecoveryPoint	Ya	Ya
AWS::Batch::ComputeEnvironment	Ya	Ya
AWS::Batch::JobQueue	Ya	Ya
AWS::Batch::SchedulingPolicy	Ya	Ya
AWS::Bedrock::Guardrail	Ya	Ya
AWS::Bedrock::KnowledgeBase	Ya	Ya
AWS::Cassandra::Keyspace	Ya	Ya
AWS::CloudFormation::Stack	Ya	Ya
AWS::CloudTrail::Trail	Ya	Ya
AWS::CloudWatch::Alarm	Ya	Ya
AWS::CodeBuild::Project	Ya	Ya

Jenis sumber daya	AWS GovCloud (AS-Barat)	AWS GovCloud (AS-Timur)
AWS::CodeBuild::ReportGroup	Ya	Ya
AWS::Cognito::IdentityPool	Ya	Tidak
AWS::Cognito::UserPoolKelompok	Ya	Tidak
AWS::Config::ConfigurationRecorder	Ya	Ya
AWS::Config::ConformancePackKepatuhan	Ya	Ya
AWS::Config::ResourceCompliance	Ya	Ya
AWS::Connect::Instance	Ya	Tidak
AWS::Connect::QuickConnect	Ya	Tidak
AWS::Connect::User	Ya	Tidak
AWS::DMS::Certificate	Ya	Ya
AWS::DMS::Endpoint	Ya	Ya
AWS::DMS::EventSubscription	Ya	Ya

Jenis sumber daya	AWS GovCloud (AS-Barat)	AWS GovCloud (AS-Timur)
AWS::DMS::ReplicationInstance	Ya	Ya
AWS::DMS::ReplicationSubnetKelompok	Ya	Ya
AWS::DMS::ReplicationTask	Ya	Ya
AWS::DataSync::LocationEFS	Ya	Ya
AWS::DataSync::LocationFSxKilau	Ya	Ya
AWS::DataSync::LocationFSxJendela	Ya	Ya
AWS::DataSync::LocationHDFS	Ya	Ya
AWS::DataSync::LocationNFS	Ya	Ya
AWS::DataSync::LocationObjectPenyimpanan	Ya	Ya
AWS::DataSync::LocationS3	Ya	Ya
AWS::DataSync::LocationSMB	Ya	Ya
AWS::DataSync::Task	Ya	Ya

Jenis sumber daya	AWS GovCloud (AS-Barat)	AWS GovCloud (AS-Timur)
AWS::Detective::Graph	Ya	Ya
AWS::DynamoDB::Table	Ya	Ya
AWS::EC2::CapacityReservation	Ya	Ya
AWS::EC2::ClientVpnTitik akhir	Ya	Ya
AWS::EC2::ClientVpnTargetNetworkAssociation	Ya	Ya
AWS::EC2::CustomerGateway	Ya	Ya
AWS::EC2:: DHCPOptions	Ya	Ya
AWS:::EC2: EC2 Armada	Ya	Ya
AWS::EC2: :EIP	Ya	Ya
AWS::EC2::EgressOnlyInternetGateway	Ya	Ya
AWS::EC2::FlowLog	Ya	Ya
AWS::EC2::Host	Ya	Ya

Jenis sumber daya	AWS GovCloud (AS-Barat)	AWS GovCloud (AS-Timur)
AWS::EC2: :IPAM	Ya	Ya
AWS::EC2:: IPAMPool	Ya	Ya
AWS::EC2:: IPAMResource Penemuan	Ya	Ya
AWS::EC2:: IPAMResource DiscoveryAssociation	Ya	Ya
AWS::EC2:: IPAMScope	Ya	Ya
AWS::EC2::Instance	Ya	Ya
AWS::EC2::InstanceConnectTitik akhir	Ya	Ya
AWS::EC2::InternetGateway	Ya	Ya
AWS::EC2::LaunchTemplate	Ya	Ya
AWS::EC2::NatGateway	Ya	Ya
AWS::EC2::NetworkAcl	Ya	Ya
AWS::EC2::NetworkInterface	Ya	Ya

Jenis sumber daya	AWS GovCloud (AS-Barat)	AWS GovCloud (AS-Timur)
AWS::EC2::PrefixList	Ya	Ya
AWS::EC2::RouteTable	Ya	Ya
AWS::EC2::SecurityGroup	Ya	Ya
AWS::EC2::SnapshotBlockPublicAccess	Ya	Ya
AWS::EC2::SpotFleet	Ya	Ya
AWS::EC2::Subnet	Ya	Ya
AWS::EC2::SubnetRouteTableAssociation	Ya	Ya
AWS::EC2::TrafficMirrorFilter	Ya	Ya
AWS::EC2::TrafficMirrorSesi	Ya	Ya
AWS::EC2::TrafficMirrorTarget	Ya	Ya
AWS::EC2::TransitGateway	Ya	Tidak
AWS::EC2::TransitGatewayLampiran	Ya	Ya

Jenis sumber daya	AWS GovCloud (AS-Barat)	AWS GovCloud (AS-Timur)
AWS::EC2::TransitGatewayConnect	Ya	Ya
AWS::EC2::TransitGatewayMulticastDomain	Ya	Ya
AWS::EC2::TransitGatewayRouteTable	Ya	Ya
AWS::EC2: :VPC	Ya	Ya
AWS::EC2:: VPCBlock PublicAccessExclusion	Ya	Ya
AWS::EC2:: VPCBlock PublicAccessOptions	Ya	Ya
AWS::EC2:: VPCEndpoint	Ya	Ya
AWS::EC2:: VPCEndpoint ConnectionNotification	Ya	Ya
AWS::EC2:: VPCEndpoint Layanan	Ya	Tidak
AWS::EC2:: VPCPeering Koneksi	Ya	Ya
AWS::EC2:: VPNConnection	Ya	Ya
AWS::EC2:: VPNConnection Rute	Ya	Ya

Jenis sumber daya	AWS GovCloud (AS-Barat)	AWS GovCloud (AS-Timur)
AWS::EC2:: VPNGateway	Ya	Ya
AWS::EC2::Volume	Ya	Ya
AWS::ECR::Repository	Ya	Ya
AWS::ECS::CapacityProvider	Ya	Ya
AWS::ECS::Cluster	Ya	Ya
AWS::ECS::Service	Ya	Ya
AWS::ECS::TaskDefinition	Ya	Ya
AWS::ECS::TaskSet	Ya	Ya
AWS::EFS::AccessPoint	Ya	Ya
AWS::EFS::FileSystem	Ya	Ya
AWS::EKS::Addon	Ya	Ya
AWS::EKS::Cluster	Ya	Ya

Jenis sumber daya	AWS GovCloud (AS-Barat)	AWS GovCloud (AS-Timur)
AWS::EKS::IdentityProviderConfig	Ya	Ya
AWS::EMR::SecurityConfiguration	Ya	Ya
AWS::ElasticBeanstalk::Application	Ya	Ya
AWS::ElasticBeanstalk::ApplicationVersion	Ya	Ya
AWS::ElasticBeanstalk::Environment	Ya	Ya
AWS::ElasticLoadBalancing::LoadBalancer	Ya	Ya
AWS::ElasticLoadBalancingV2::Listener	Ya	Ya
AWS::ElasticLoadBalancingV2::LoadBalancer	Ya	Ya
AWS::Elasticsearch::Domain	Ya	Ya
AWS::Events::EventBus	Ya	Ya
AWS::Events::Rule	Ya	Ya
AWS::FIS::ExperimentTemplate	Ya	Ya

Jenis sumber daya	AWS GovCloud (AS-Barat)	AWS GovCloud (AS-Timur)
AWS::Glue::Classifier	Ya	Ya
AWS::Glue::Job	Ya	Ya
AWS::Glue::MLTransform	Ya	Tidak
AWS::GreengrassV2::ComponentVersion	Ya	Ya
AWS::GuardDuty::Detector	Ya	Ya
AWS::GuardDuty::Filter	Ya	Ya
AWS::GuardTugas:: IPSet	Ya	Ya
AWS::GuardDuty::ThreatIntelSet	Ya	Ya
AWS::IAM::Group	Ya	Ya
AWS::IAM::InstanceProfile	Tidak	Ya
AWS: :IAM:: OIDCProvider	Tidak	Ya
AWS::IAM::Policy	Ya	Ya

Jenis sumber daya	AWS GovCloud (AS-Barat)	AWS GovCloud (AS-Timur)
AWS::IAM::Role	Ya	Ya
AWS: :IAM:: SAMLProvider	Tidak	Ya
AWS::IAM::ServerCertificate	Tidak	Ya
AWS::IAM::User	Ya	Ya
AWS::ImageBuilder::ContainerRecipe	Ya	Ya
AWS::ImageBuilder::DistributionConfiguration	Ya	Ya
AWS::ImageBuilder::ImagePipeline	Ya	Ya
AWS::ImageBuilder::ImageRecipe	Ya	Ya
AWS::ImageBuilder::InfrastructureConfiguration	Ya	Ya
AWS::InspectorV2::Activation	Ya	Ya
AWS::IoT::AccountAuditKonfigurasi	Ya	Ya
AWS::IoT::Authorizer	Ya	Ya

Jenis sumber daya	AWS GovCloud (AS-Barat)	AWS GovCloud (AS-Timur)
AWS::IoT:: CACertificate	Ya	Ya
AWS::IoT::CustomMetric	Ya	Ya
AWS::IoT::Dimension	Ya	Ya
AWS::IoT::FleetMetric	Ya	Ya
AWS::IoT::JobTemplate	Ya	Ya
AWS::IoT::MitigationAction	Ya	Ya
AWS::IoT::Policy	Ya	Ya
AWS::IoT::ProvisioningTemplate	Ya	Ya
AWS::IoT::RoleAlias	Ya	Ya
AWS::IoT::ScheduledAudit	Ya	Ya
AWS::IoT::SecurityProfile	Ya	Ya
AWS::IoTEvents::AlarmModel	Ya	Tidak

Jenis sumber daya	AWS GovCloud (AS-Barat)	AWS GovCloud (AS-Timur)
AWS::IoTEvents::DetectorModel	Ya	Tidak
AWS::IoTEvents::Input	Ya	Tidak
AWS::IoTSiteWise::AssetModel	Ya	Tidak
AWS::IoTSiteWise::Gateway	Ya	Tidak
AWS::IoTSiteWise::Portal	Ya	Tidak
AWS::IoTTwinMaker::ComponentType	Ya	Tidak
AWS::IoTTwinMaker::Entity	Ya	Tidak
AWS::IoTTwinMaker::Workspace	Ya	Tidak
AWS::KMS::Alias	Ya	Ya
AWS::KMS::Key	Ya	Ya
AWS::Kinesis::Stream	Ya	Ya
AWS::Kinesis::StreamConsumer	Ya	Ya

Jenis sumber daya	AWS GovCloud (AS-Barat)	AWS GovCloud (AS-Timur)
AWS::KinesisAnalyticsV2::Application	Ya	Ya
AWS::KinesisFirehose::DeliveryStream	Ya	Ya
AWS::Lambda::Function	Ya	Ya
AWS::Logs::Destination	Ya	Ya
AWS::MSK::BatchScramRahasia	Ya	Ya
AWS::MSK::Cluster	Ya	Ya
AWS::MSK::ClusterPolicy	Ya	Ya
AWS::MSK::Configuration	Ya	Ya
AWS::MSK::VpcConnection	Ya	Ya
AWS::NetworkFirewall::Firewall	Ya	Ya
AWS::NetworkFirewall::FirewallPolicy	Ya	Ya
AWS::NetworkFirewall::RuleGroup	Ya	Ya

Jenis sumber daya	AWS GovCloud (AS-Barat)	AWS GovCloud (AS-Timur)
AWS::NetworkFirewall::VpcEndpointAsosiasi	Ya	Ya
AWS::NetworkManager::CustomerGatewayAsosiasi	Ya	Tidak
AWS::NetworkManager::Device	Ya	Tidak
AWS::NetworkManager::GlobalNetwork	Ya	Tidak
AWS::NetworkManager::Link	Ya	Tidak
AWS::NetworkManager::LinkAssociation	Ya	Tidak
AWS::NetworkManager::Site	Ya	Tidak
AWS::NetworkManager::TransitGatewayRegistrasi	Ya	Tidak
AWS::OpenSearch::Domain	Ya	Ya
AWS::Pinpoint::App	Ya	Tidak
AWS::Pinpoint::ApplicationSettings	Ya	Tidak
AWS::Pinpoint::Campaign	Ya	Tidak

Jenis sumber daya	AWS GovCloud (AS-Barat)	AWS GovCloud (AS-Timur)
AWS::Pinpoint::EmailChannel	Ya	Tidak
AWS::Pinpoint::EmailTemplate	Ya	Tidak
AWS::Pinpoint::EventStream	Ya	Tidak
AWS::Pinpoint::InAppTemplate	Ya	Tidak
AWS::Pinpoint::Segment	Ya	Tidak
AWS::QuickSight::Template	Ya	Tidak
AWS: :RDS:: DBCluster	Ya	Ya
AWS: :RDS:: Snapshot DBCluster	Ya	Ya
AWS: :RDS:: DBInstance	Ya	Ya
AWS: :RDS:: Grup DBSecurity	Ya	Ya
AWS: :RDS:: DBSnapshot	Ya	Ya
AWS: :RDS:: Grup DBSubnet	Ya	Ya

Jenis sumber daya	AWS GovCloud (AS-Barat)	AWS GovCloud (AS-Timur)
AWS::RDS::EventSubscription	Ya	Ya
AWS::RDS::OptionGroup	Ya	Ya
AWS::Redshift::Cluster	Ya	Ya
AWS::Redshift::ClusterParameterKelompok	Ya	Ya
AWS::Redshift::ClusterSecurityKelompok	Ya	Ya
AWS::Redshift::ClusterSnapshot	Ya	Ya
AWS::Redshift::ClusterSubnetKelompok	Ya	Ya
AWS::Redshift::EventSubscription	Ya	Ya
AWS::Redshift::ScheduledAction	Ya	Ya
AWS::RoboMaker::RobotApplication	Ya	Tidak
AWS::RoboMaker::RobotApplicationVersi	Ya	Tidak
AWS::RoboMaker::SimulationApplication	Ya	Tidak

Jenis sumber daya	AWS GovCloud (AS-Barat)	AWS GovCloud (AS-Timur)
AWS::Route53Profiles::Profile	Ya	Ya
AWS::Route53Resolver::FirewallDomainDaftar	Ya	Ya
AWS::Route53Resolver::FirewallRuleKelompok	Ya	Ya
AWS::Route53Resolver::FirewallRuleGroupAssociation	Ya	Ya
AWS::Route53Resolver::ResolverEndpoint	Ya	Ya
AWS::Route53Resolver::ResolverQueryLoggingConfig	Ya	Ya
AWS::Route53Resolver::Resol verQueryLoggingConfigAssociation	Ya	Ya
AWS::Route53Resolver::ResolverRule	Ya	Ya
AWS::Route53Resolver::ResolverRuleAsosiasi	Ya	Ya
AWS::S3::AccessPoint	Ya	Ya
AWS::S3::AccountPublicAccessBlock	Ya	Ya
AWS::S3::Bucket	Ya	Ya

Jenis sumber daya	AWS GovCloud (AS-Barat)	AWS GovCloud (AS-Timur)
AWS::SES::ConfigurationSet	Ya	Tidak
AWS::SES::ContactList	Ya	Tidak
AWS::SES::Template	Ya	Tidak
AWS::SNS::Topic	Ya	Ya
AWS::SQS::Queue	Ya	Ya
AWS::SSM::AssociationCompliance	Ya	Ya
AWS::SSM::Document	Ya	Ya
AWS::SSM::FileData	Ya	Ya
AWS::SSM::ManagedInstanceInventaris	Ya	Ya
AWS::SSM::PatchCompliance	Ya	Ya
AWS::SageMaker::Model	Ya	Tidak
AWS::SageMaker::NotebookInstance	Ya	Tidak

Jenis sumber daya	AWS GovCloud (AS-Barat)	AWS GovCloud (AS-Timur)
AWS::SageMaker::NotebookInstanceLifecycleConfig	Ya	Tidak
AWS::SecretsManager::Secret	Ya	Ya
AWS::SecurityHub::Standard	Ya	Ya
AWS::ServiceCatalog::CloudFormationProduk	Ya	Ya
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Ya	Ya
AWS::ServiceCatalog::Portfolio	Ya	Ya
AWS::ServiceDiscovery::HttpNamespace	Ya	Ya
AWS::ServiceDiscovery::Instance	Ya	Ya
AWS::ServiceDiscovery::Service	Ya	Ya
AWS::StepFunctions::StateMachine	Ya	Ya
AWS::Transfer::Agreement	Ya	Ya
AWS::Transfer::Certificate	Ya	Ya

Jenis sumber daya	AWS GovCloud (AS-Barat)	AWS GovCloud (AS-Timur)
AWS::Transfer::Connector	Ya	Ya
AWS::Transfer::Profile	Ya	Ya
AWS::Transfer::Workflow	Ya	Ya
AWS::WAFRegional::RateBasedAturan	Ya	Ya
AWS::WAFRegional::Rule	Ya	Ya
AWS::WAFRegional::RuleGroup	Ya	Ya
AWS::WAFRegional::WebACL	Ya	Ya
AWS::WAFv2:: IPSet	Ya	Ya
AWS::WAFv2::ManagedRuleSet	Ya	Ya
AWS::WAFv2::RegexPatternSet	Ya	Ya
AWS::WAFv2::RuleGroup	Ya	Ya
AWS::WAFv2::WebACL	Ya	Ya

Jenis sumber daya	AWS GovCloud (AS-Barat)	AWS GovCloud (AS-Timur)
AWS::WorkSpaces::Workspace	Ya	Tidak

Merekam AWS Sumber Daya dengan AWS Config

AWS Config terus mendeteksi kapan jenis sumber daya yang didukung dibuat, diubah, atau dihapus. AWS Config mencatat peristiwa ini sebagai item konfigurasi (CIs).

Anda dapat menyesuaikan AWS Config untuk merekam perubahan konfigurasi untuk semua jenis sumber daya yang didukung, atau hanya untuk jenis sumber daya yang didukung yang relevan bagi Anda. Untuk daftar jenis sumber daya yang didukung yang AWS Config dapat merekam, lihatJenis Sumber Daya yang Didukung untuk AWS Config.

Topik

- Pertimbangan
- Apa perbedaan antara sumber daya regional dan global?
- AWS Config Aturan dan jenis sumber daya global
- Frekuensi perekaman untuk AWS Config
- Sumber daya yang tidak direkam
- Merekam sumber daya di AWS Config konsol
- Merekam sumber daya dengan AWS CLI
- Mengecualikan sumber daya dari perekaman dengan AWS Config
- AWS Config Berhenti merekam dengan perekam konfigurasi terkelola pelanggan

Pertimbangan

Jumlah AWS Config Evaluasi yang Tinggi

Anda mungkin melihat peningkatan aktivitas di akun selama perekaman bulan awal dengan AWS Config jika dibandingkan dengan bulan-bulan berikutnya. Selama proses bootstrap awal, AWS Config

jalankan evaluasi pada semua sumber daya di akun Anda yang telah Anda pilih untuk direkam. AWS Config

Jika Anda menjalankan beban kerja sementara, Anda mungkin melihat peningkatan aktivitas dari AWS Config saat merekam perubahan konfigurasi yang terkait dengan pembuatan dan penghapusan sumber daya sementara ini. Beban kerja sementara adalah penggunaan sementara sumber daya komputasi yang dimuat dan dijalankan saat diperlukan. Contohnya termasuk Instans Spot Amazon Elastic Compute Cloud (Amazon EC2), pekerjaan EMR Amazon, dan. AWS Auto Scaling

Jika Anda ingin menghindari peningkatan aktivitas menjalankan beban kerja sementara, Anda dapat mengatur perekam konfigurasi terkelola pelanggan untuk mengecualikan jenis sumber daya ini agar tidak direkam, atau menjalankan jenis beban kerja ini di akun terpisah dengan AWS Config dimatikan untuk menghindari peningkatan perekaman konfigurasi dan evaluasi aturan.

Ketersediaan Wilayah

Sebelum menentukan jenis sumber daya AWS Config untuk dilacak, periksa Cakupan Sumber Daya menurut ketersediaan Wilayah untuk melihat apakah jenis sumber daya didukung di AWS Wilayah tempat Anda menyiapkan AWS Config.

Jika jenis sumber daya didukung oleh AWS Config setidaknya satu Wilayah, Anda dapat mengaktifkan perekaman jenis sumber daya tersebut di semua Wilayah yang didukung oleh AWS Config, meskipun jenis sumber daya yang ditentukan tidak didukung di AWS Wilayah tempat Anda menyiapkan AWS Config.

Apa perbedaan antara sumber daya regional dan global?

Sumber daya regional

Sumber daya regional terikat pada suatu Wilayah dan hanya dapat digunakan di Wilayah tersebut. Anda membuatnya dalam yang ditentukan Wilayah AWS, dan kemudian mereka ada di Wilayah itu. Untuk melihat atau berinteraksi dengan sumber daya tersebut, Anda harus mengarahkan operasi Anda ke Wilayah tersebut. Misalnya, untuk membuat EC2 instance Amazon dengan AWS Management Console, Anda memilih instans Wilayah AWS yang ingin Anda buat. Jika Anda menggunakan AWS Command Line Interface (AWS CLI) untuk membuat instance, maka Anda menyertakan `--region` parameter. AWS SDKs Masing-masing memiliki mekanisme ekuivalennya sendiri untuk menentukan Wilayah yang digunakan operasi.

Ada beberapa alasan untuk menggunakan sumber daya Regional. Salah satu alasannya adalah untuk memastikan bahwa sumber daya, dan titik akhir layanan yang Anda gunakan

untuk mengaksesnya, sedekat mungkin dengan pelanggan. Ini meningkatkan kinerja dengan meminimalkan latensi. Alasan lain adalah untuk memberikan batas isolasi. Ini memungkinkan Anda membuat salinan sumber daya independen di beberapa Wilayah untuk mendistribusikan beban dan meningkatkan skalabilitas. Pada saat yang sama, ia mengisolasi sumber daya satu sama lain untuk meningkatkan ketersediaan.

Jika Anda menentukan yang berbeda Wilayah AWS di konsol atau dalam AWS CLI perintah, maka Anda tidak dapat lagi melihat atau berinteraksi dengan sumber daya yang dapat Anda lihat di Wilayah sebelumnya.

Saat Anda melihat Nama Sumber Daya Amazon (ARN) untuk sumber daya Regional, Wilayah yang berisi sumber daya ditentukan sebagai bidang keempat di ARN. Misalnya, EC2 instans Amazon adalah sumber daya Regional. Berikut ini adalah contoh ARN untuk EC2 instance Amazon yang ada di Wilayah. `us-east-1`

```
arn:aws:ec2:us-east-1:123456789012:instance/i-0a6f30921424d3eee
```

Sumber daya global

Beberapa sumber daya AWS layanan adalah sumber daya global, artinya Anda dapat menggunakan sumber daya dari mana saja. Anda tidak menentukan Wilayah AWS di konsol layanan global. Untuk mengakses sumber daya global, Anda tidak menentukan `--region` parameter saat menggunakan operasi layanan AWS CLI dan AWS SDK.

Sumber daya global mendukung kasus di mana sangat penting bahwa hanya satu contoh sumber daya tertentu yang dapat eksis pada satu waktu. Dalam skenario ini, replikasi atau sinkronisasi antar salinan di Wilayah yang berbeda tidak memadai. Harus mengakses satu titik akhir global, dengan kemungkinan peningkatan latensi, dianggap dapat diterima untuk memastikan bahwa setiap perubahan langsung terlihat oleh konsumen sumber daya.

Misalnya, klaster global Amazon Aurora (`AWS::RDS::GlobalCluster`) adalah sumber daya global, dan karenanya tidak terikat pada suatu Wilayah. Ini berarti Anda dapat membuat cluster global tanpa bergantung pada titik akhir regional. Manfaatnya adalah, sementara Amazon Relational Database Service (Amazon RDS) sendiri diatur oleh Wilayah, Wilayah spesifik tempat cluster global berasal tidak berdampak pada cluster global. Ini muncul sebagai cluster global tunggal yang berkelanjutan di semua Wilayah.

Nama Sumber Daya Amazon (ARN) untuk sumber daya global tidak menyertakan Wilayah. Bidang keempat kosong, seperti pada contoh ARN berikut untuk cluster global.

```
arn:aws:rds::123456789012:global-cluster:test-global-cluster
```

> **Important**
>
> Jenis sumber daya global yang tersedia AWS Config setelah Februari 2022 hanya akan dicatat di Wilayah asal layanan untuk partisi komersial dan AWS GovCloud (AS-Barat) untuk partisi tersebut. GovCloud Anda dapat melihat item konfigurasi (CIs) untuk jenis sumber daya global baru ini hanya di wilayah asal mereka dan AWS GovCloud (AS-Barat).
>
> Jenis sumber daya global yang tersedia sebelum Februari 2022 (`AWS::IAM::Group`,, `AWS::IAM::PolicyAWS::IAM::Role`, dan`AWS::IAM::User`) tetap tidak berubah. Anda dapat mengaktifkan perekaman sumber daya IAM global ini di semua Wilayah yang AWS Config didukung sebelum Februari 2022. Sumber daya IAM global ini tidak dapat dicatat di Wilayah yang didukung AWS Config setelah Februari 2022.

Jenis sumber daya global | Sumber daya IAM

Jenis sumber daya IAM berikut adalah sumber daya global: pengguna IAM, grup, peran, dan kebijakan yang dikelola pelanggan. Jenis sumber daya ini dapat direkam oleh AWS Config di Wilayah AWS Config yang tersedia sebelum Februari 2022. Daftar ini di mana Anda tidak dapat merekam jenis sumber daya IAM global mencakup Wilayah berikut: Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Asia Pasifik (Thailand), Kanada Barat (Calgary), Eropa (Spanyol), Eropa (Zurich), Israel (Tel Aviv), Meksiko (Tengah), dan Timur Tengah (UEA).

Untuk mencegah duplikat item konfigurasi (CIs), Anda harus mempertimbangkan hanya merekam jenis sumber daya IAM global satu kali di salah satu Wilayah yang didukung. Ini juga dapat membantu Anda menghindari evaluasi yang tidak perlu dan pembatasan API.

Jenis sumber daya global | Hanya Wilayah Beranda

Sumber daya global untuk layanan berikut hanya dicatat oleh AWS Config Wilayah asal dari jenis sumber daya global: Amazon Elastic Container Registry Public, AWS Global Accelerator, Amazon Route 53, Amazon CloudFront, dan AWS WAF. Untuk sumber daya global ini, contoh yang sama dari jenis sumber daya dapat digunakan di beberapa AWS Wilayah, tetapi item konfigurasi (CIs) hanya dicatat di Wilayah asal untuk partisi komersial atau AWS GovCloud (AS-Barat) untuk AWS GovCloud (US) partisi.

Beranda Wilayah untuk Jenis Sumber Daya Global

AWS Layanan	Nilai Jenis Sumber Daya	Wilayah Asal
Amazon Elastic Container Registry Publik	`AWS::ECR::PublicRepository`	Wilayah AS Timur (Virginia Utara)
AWS Global Accelerator	`AWS::GlobalAccelerator::Listener`	Wilayah AS Barat (Oregon)
	`AWS::GlobalAccelerator::EndpointGroup`	Wilayah AS Barat (Oregon)
	`AWS::GlobalAccelerator::Accelerator`	Wilayah AS Barat (Oregon)
Amazon Route 53	`AWS::Route53::HostedZone`	Wilayah AS Timur (Virginia Utara)
	`AWS::Route53::HealthCheck`	Wilayah AS Timur (Virginia Utara)
Amazon CloudFront	`AWS::CloudFront::Distribution`	Wilayah AS Timur (Virginia Utara)
AWS WAF	`AWS::WAFv2::WebACL`	Wilayah AS Timur (Virginia Utara)

Jenis sumber daya global | Kluster global Aurora

`AWS::RDS::GlobalCluster`adalah sumber daya global yang direkam di semua AWS Config Wilayah yang didukung tempat perekam konfigurasi terkelola pelanggan diaktifkan. Jenis sumber daya global ini unik karena jika Anda mengaktifkan perekaman sumber daya ini dalam satu Wilayah, AWS Config akan merekam item konfigurasi (CIs) untuk jenis sumber daya ini di semua Wilayah yang diaktifkan.

Jika Anda tidak ingin merekam `AWS::RDS::GlobalCluster` di semua Wilayah yang diaktifkan, gunakan salah satu strategi perekaman berikut untuk AWS Config konsol:

- Rekam semua jenis sumber daya dengan penggantian yang dapat disesuaikan, pilih "AWS RDS GlobalCluster “, dan pilih penggantian “Kecualikan dari perekaman”
- Rekam jenis sumber daya tertentu.

Jika Anda tidak ingin merekam `AWS::RDS::GlobalCluster` di semua Wilayah yang diaktifkan, gunakan salah satu strategi perekaman berikut untuk API/CLI:

- Rekam semua jenis sumber daya saat ini dan masa depan dengan pengecualian () `EXCLUSION_BY_RESOURCE_TYPES`
- Rekam jenis sumber daya tertentu (`INCLUSION_BY_RESOURCE_TYPES`).

AWS Config Aturan dan jenis sumber daya global

Jenis sumber daya IAM global yang tersedia sebelum Februari 2022 (`AWS::IAM::Group`,, `AWS::IAM::Policy`AWS::IAM::Role, dan`AWS::IAM::User`) hanya dapat direkam oleh AWS Config di Wilayah yang tersedia sebelum AWS Config Februari 2022. Jenis sumber daya IAM global ini tidak dapat dicatat di Wilayah yang didukung AWS Config setelah Februari 2022. Untuk daftar Wilayah tersebut, lihat Merekam AWS Sumber Daya | Sumber Daya Global.

Jika Anda merekam jenis sumber daya IAM global di setidaknya satu Wilayah, aturan periodik yang melaporkan kepatuhan pada jenis sumber daya IAM global akan menjalankan evaluasi di semua Wilayah di mana aturan periodik ditambahkan, bahkan jika Anda belum mengaktifkan pencatatan jenis sumber daya IAM global di Wilayah tempat aturan periodik ditambahkan.

Praktik Terbaik untuk melaporkan kepatuhan terhadap sumber daya global yang tersedia sebelum Februari 2022

Untuk menghindari evaluasi yang tidak perlu, Anda hanya harus menerapkan AWS Config aturan dan paket kesesuaian yang memiliki sumber daya global ini dalam cakupan ke salah satu Wilayah yang didukung. Untuk daftar aturan terkelola yang didukung di Wilayah mana, lihat Daftar Aturan AWS Config Terkelola menurut Ketersediaan Wilayah. Ini berlaku untuk AWS Config aturan, AWS Config aturan organisasi, dan juga aturan yang dibuat oleh AWS layanan lain, seperti AWS Security Hub dan AWS Control Tower.

Jika Anda tidak merekam jenis sumber daya global yang tersedia sebelum Februari 2022, Anda disarankan untuk tidak mengaktifkan aturan berkala berikut untuk menghindari evaluasi yang tidak perlu:

- access-keys-rotated

- account-part-of-organizations
- iam-password-policy
- iam-policy-in-use
- iam-root-access-key-periksa
- iam-user-mfa-enabled
- iam-user-unused-credentials-periksa
- mfa-enabled-for-iam-akses konsol
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled

Praktik Terbaik untuk melaporkan kepatuhan terhadap sumber daya global yang tersedia setelah Februari 2022

Jenis sumber daya global yang dimasukkan ke dalam AWS Config rekaman setelah Februari 2022 hanya akan direkam di Wilayah asal layanan untuk partisi komersial dan AWS GovCloud (AS-Barat) untuk partisi. AWS GovCloud (US) Anda harus menerapkan AWS Config aturan dan paket kesesuaian yang memiliki sumber daya global ini dalam cakupan hanya untuk Wilayah asal tipe sumber daya. Untuk informasi selengkapnya, lihat Wilayah Beranda untuk Jenis Sumber Daya Global.

Frekuensi perekaman untuk AWS Config

AWS Config mendukung perekaman berkelanjutan dan perekaman harian. Perekaman berkelanjutan memungkinkan Anda merekam perubahan konfigurasi secara terus menerus setiap kali terjadi perubahan. Rekaman harian memungkinkan Anda menerima item konfigurasi (CI) yang mewakili status terbaru sumber daya Anda selama periode 24 jam terakhir, hanya jika berbeda dari CI sebelumnya yang direkam. Untuk langkah-langkah tentang cara mengubah frekuensi perekaman, lihat Mengubah Frekuensi Perekaman.

Perekaman terus menerus

Beberapa manfaat perekaman berkelanjutan meliputi:

- Pemantauan Real-time: Perekaman berkelanjutan dapat memberikan deteksi langsung untuk perubahan yang tidak sah atau perubahan tak terduga, yang dapat meningkatkan upaya keamanan dan kepatuhan Anda.

- Analisis Terperinci: Perekaman berkelanjutan dapat memungkinkan Anda melakukan analisis mendalam tentang perubahan konfigurasi pada sumber daya Anda saat terjadi, yang memungkinkan Anda mengidentifikasi pola dan tren saat ini.

Rekaman harian

Beberapa manfaat perekaman harian meliputi:

- Gangguan Minimal: Rekaman harian dapat memberi Anda aliran informasi yang lebih mudah ditangani, yang dapat mengurangi frekuensi pemberitahuan dan kelelahan peringatan.
- Efisiensi Biaya: Rekaman harian dapat memberi Anda fleksibilitas untuk merekam perubahan pada sumber daya Anda pada frekuensi yang lebih rendah, yang dapat mengurangi biaya yang terkait dengan jumlah perubahan konfigurasi yang direkam.

> **Note**
>
> AWS Firewall Manager tergantung pada perekaman berkelanjutan untuk memantau sumber daya Anda. Jika Anda menggunakan Firewall Manager, disarankan agar Anda mengatur frekuensi perekaman ke Continuous.

Sumber daya yang tidak direkam

Jika sumber daya tidak direkam, hanya AWS Config menangkap pembuatan dan penghapusan sumber daya itu, dan tidak ada detail lainnya, tanpa biaya kepada Anda. Ketika sumber daya yang tidak direkam dibuat atau dihapus, AWS Config mengirimkan pemberitahuan, dan menampilkan acara di halaman detail sumber daya. Halaman detail untuk sumber daya yang tidak direkam memberikan nilai nol untuk sebagian besar detail konfigurasi, dan tidak memberikan informasi tentang hubungan dan perubahan konfigurasi.

Informasi hubungan yang AWS Config menyediakan sumber daya yang direkam tidak terbatas karena data yang hilang untuk sumber daya yang tidak direkam. Jika sumber daya yang direkam terkait dengan sumber daya yang tidak direkam, hubungan itu disediakan di halaman detail sumber daya yang direkam.

Pertimbangan tipe sumber daya IAM

Jenis `AWS::IAM::Role` sumber daya `AWS::IAM::User` `AWS::IAM::Policy` `AWS::IAM::Group`,,, hanya akan menangkap status creation (`ResourceNotRecorded`) dan deletion (`ResourceDeletedNotRecorded`) jika sumber daya, atau sebelumnya, dipilih sebagai sumber daya untuk direkam dalam perekam konfigurasi terkelola pelanggan.

Jadwal perekaman CI untuk sumber daya yang tidak direkam

Item konfigurasi (CIs) untuk `ResourceNotRecorded` dan `ResourceDeletedNotRecorded` tidak mengikuti waktu perekaman khas untuk jenis sumber daya. Jenis sumber daya ini hanya dicatat selama proses baselining berkala untuk perekam konfigurasi yang dikelola pelanggan, yang pada irama yang lebih jarang daripada jenis sumber daya lainnya. Ini berarti bahwa notifikasi buat dan hapus tidak dikirim pada saat pembuatan atau penghapusan, tetapi selama proses baselining.

Pengiriman CI dan lingkup perekam terkait layanan

Untuk perekam konfigurasi terkait layanan, cakupan perekaman menentukan apakah Anda menerima item konfigurasi (CIs) di saluran pengiriman. Lingkup perekaman diatur oleh layanan yang ditautkan ke perekam konfigurasi. Jika ruang lingkup perekaman internal, Anda tidak akan menerima CIs di saluran pengiriman.

Merekam sumber daya di AWS Config konsol

Anda dapat menggunakan AWS Config konsol untuk memilih jenis sumber daya yang AWS Config direkam dengan perekam konfigurasi terkelola pelanggan.

Untuk memilih sumber daya

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Pilih Pengaturan di panel navigasi kiri.
3. Pada tab Perekam terkelola pelanggan, pilih Edit.
4. Di bagian Metode perekaman, pilih strategi perekaman. Anda dapat menentukan AWS sumber daya yang AWS Config ingin Anda rekam.

   All resource types with customizable overrides

   Siapkan AWS Config untuk merekam perubahan konfigurasi untuk semua jenis sumber daya yang didukung saat ini dan masa depan di Wilayah ini. Anda dapat mengganti frekuensi perekaman untuk jenis sumber daya tertentu atau mengecualikan jenis sumber daya tertentu dari perekaman. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.

- Pengaturan default

  Konfigurasikan frekuensi perekaman default untuk semua jenis sumber daya yang didukung saat ini dan masa depan. Untuk informasi lebih lanjut lihat, Frekuensi Perekaman.

  - Perekaman berkelanjutan - AWS Config akan merekam perubahan konfigurasi secara terus menerus setiap kali terjadi perubahan.
  - Rekaman harian — Anda akan menerima item konfigurasi (CI) yang mewakili status terbaru sumber daya Anda selama periode 24 jam terakhir, hanya jika berbeda dari CI sebelumnya yang direkam.

  > **Note**
  >
  > AWS Firewall Manager tergantung pada perekaman berkelanjutan untuk memantau sumber daya Anda. Jika Anda menggunakan Firewall Manager, disarankan agar Anda mengatur frekuensi perekaman ke Continuous.

- Ganti pengaturan

  Ganti frekuensi perekaman untuk jenis sumber daya tertentu, atau kecualikan jenis sumber daya tertentu dari perekaman. Jika Anda mengubah frekuensi perekaman untuk jenis sumber daya atau berhenti merekam jenis sumber daya, item konfigurasi yang sudah direkam akan tetap tidak berubah.

Specific resource types

Siapkan AWS Config untuk merekam perubahan konfigurasi hanya untuk jenis sumber daya yang Anda tentukan.

- Jenis sumber daya tertentu

  Pilih jenis sumber daya untuk merekam dan frekuensinya. Untuk informasi lebih lanjut lihat, Frekuensi Perekaman.

  - Perekaman berkelanjutan - AWS Config akan merekam perubahan konfigurasi secara terus menerus setiap kali terjadi perubahan.
  - Rekaman harian — Anda akan menerima item konfigurasi (CI) yang mewakili status terbaru sumber daya Anda selama periode 24 jam terakhir, hanya jika berbeda dari CI sebelumnya yang direkam.

> **Note**
>
> AWS Firewall Manager tergantung pada perekaman berkelanjutan untuk memantau sumber daya Anda. Jika Anda menggunakan Firewall Manager, disarankan agar Anda mengatur frekuensi perekaman ke Continuous.

Jika Anda mengubah frekuensi perekaman untuk jenis sumber daya atau berhenti merekam jenis sumber daya, item konfigurasi yang sudah direkam akan tetap tidak berubah.

5. Pilih Simpan untuk menyimpan perubahan Anda.

Pertimbangan Saat Merekam Sumber Daya

Jumlah AWS Config Evaluasi yang Tinggi

Anda mungkin melihat peningkatan aktivitas di akun selama perekaman bulan awal dengan AWS Config jika dibandingkan dengan bulan-bulan berikutnya. Selama proses bootstrap awal, AWS Config jalankan evaluasi pada semua sumber daya di akun Anda yang telah Anda pilih untuk direkam. AWS Config

Jika Anda menjalankan beban kerja sementara, Anda mungkin melihat peningkatan aktivitas dari AWS Config saat merekam perubahan konfigurasi yang terkait dengan pembuatan dan penghapusan sumber daya sementara ini. Beban kerja sementara adalah penggunaan sementara sumber daya komputasi yang dimuat dan dijalankan saat diperlukan. Contohnya termasuk Instans Spot Amazon Elastic Compute Cloud (Amazon EC2), pekerjaan EMR Amazon, dan. AWS Auto Scaling Jika Anda ingin menghindari peningkatan aktivitas menjalankan beban kerja sementara, Anda dapat mengatur perekam konfigurasi terkelola pelanggan untuk mengecualikan jenis sumber daya ini agar tidak direkam, atau menjalankan jenis beban kerja ini di akun terpisah dengan AWS Config dimatikan untuk menghindari peningkatan perekaman konfigurasi dan evaluasi aturan.

Considerations: All resource types with customizable overrides

Jenis sumber daya yang direkam secara global | Kluster global Aurora pada awalnya disertakan dalam rekaman

Jenis `AWS::RDS::GlobalCluster` sumber daya akan direkam di semua AWS Config Wilayah yang didukung tempat perekam konfigurasi terkelola pelanggan diaktifkan.

Jika Anda tidak ingin merekam `AWS::RDS::GlobalCluster` di semua Wilayah yang diaktifkan, pilih "AWS RDS GlobalCluster“, dan pilih penggantian “Kecualikan dari perekaman”.

Jenis sumber daya global | Jenis sumber daya IAM awalnya dikecualikan dari perekaman

Jenis sumber daya IAM global pada awalnya dikecualikan dari pencatatan untuk membantu Anda mengurangi biaya. Paket ini mencakup pengguna IAM, grup, peran, dan kebijakan yang dikelola pelanggan. Pilih Hapus untuk menghapus penggantian dan menyertakan sumber daya ini dalam rekaman Anda.

Selain itu, jenis sumber daya IAM global (`AWS::IAM::User`,`AWS::IAM::Group`,`AWS::IAM::Role`, dan`AWS::IAM::Policy`) tidak dapat dicatat di Wilayah yang didukung AWS Config setelah Februari 2022. Untuk daftar Wilayah tersebut, lihat Merekam AWS Sumber Daya | Sumber Daya Global.

Batas

Anda dapat menambahkan hingga 100 penggantian frekuensi dan 600 penggantian pengecualian.

Rekaman harian tidak didukung untuk jenis sumber daya berikut:

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

Considerations: Specific resource types

Ketersediaan Wilayah

Sebelum menentukan jenis sumber daya AWS Config untuk dilacak, periksa Cakupan Sumber Daya menurut Ketersediaan Wilayah untuk melihat apakah jenis sumber daya didukung di AWS Wilayah tempat Anda menyiapkan AWS Config. Jika jenis sumber daya didukung oleh AWS Config setidaknya satu Wilayah, Anda dapat mengaktifkan perekaman jenis sumber daya tersebut di semua Wilayah yang didukung oleh AWS Config, meskipun jenis sumber daya yang ditentukan tidak didukung di AWS Wilayah tempat Anda menyiapkan AWS Config.

Batas

Tidak ada batasan jika semua jenis sumber daya memiliki frekuensi yang sama. Anda dapat menambahkan hingga 100 jenis sumber daya dengan frekuensi Harian jika setidaknya satu jenis sumber daya diatur ke Continuous.

Frekuensi harian tidak didukung untuk jenis sumber daya berikut:

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

Merekam sumber daya dengan AWS CLI

Anda dapat menggunakan AWS CLI untuk memilih jenis sumber daya yang AWS Config ingin Anda rekam. Anda melakukannya dengan membuat perekam konfigurasi terkelola pelanggan, yang merekam jenis sumber daya yang Anda tentukan dalam grup rekaman. Dalam grup rekaman, Anda menentukan apakah Anda ingin merekam semua jenis sumber daya yang didukung, atau untuk menyertakan atau mengecualikan jenis sumber daya tertentu.

Record all current and future supported resource types

Siapkan AWS Config untuk merekam perubahan konfigurasi untuk semua jenis sumber daya yang didukung saat ini dan masa depan di Wilayah ini. Untuk daftar jenis sumber daya yang didukung, lihat Jenis Sumber Daya yang Didukung.

1. Gunakan `put-configuration-recorder`perintah:

   Perintah ini menggunakan `--configuration-recorder` dan `---recording-group` bidang.

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

   `configuration-recorder`Bidang

   `configurationRecorder.json`File menentukan `name` dan `roleArn` serta frekuensi perekaman default untuk perekam konfigurasi (`recordingMode`).

   ```
   {
   ```

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

`recording-group`Bidang

`recordingGroup.json`File menentukan jenis sumber daya yang direkam.

```
{
    "allSupported": true,
    "recordingStrategy": {
        "useOnly": "ALL_SUPPORTED_RESOURCE_TYPES"
    },
    "includeGlobalResourceTypes": true
}
```

Untuk informasi selengkapnya tentang bidang ini, lihat `put-configuration-recorder`di Referensi AWS CLI Perintah.

2. (Opsional) Untuk memverifikasi bahwa perekam konfigurasi terkelola pelanggan Anda memiliki pengaturan yang Anda inginkan, gunakan `describe-configuration-recorders`perintah berikut.

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

Berikut ini adalah contoh respons.

```
{
    "ConfigurationRecorders": [
        {
```

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

Record all current and future supported resources types excluding the types you specify

Siapkan AWS Config untuk merekam perubahan konfigurasi untuk semua jenis sumber daya yang didukung saat ini dan masa depan, termasuk tipe sumber daya global, kecuali jenis sumber daya yang Anda tentukan untuk dikecualikan dari rekaman.

Jika Anda memilih untuk berhenti merekam untuk jenis sumber daya, item konfigurasi yang sudah direkam akan tetap tidak berubah. Untuk daftar jenis sumber daya yang didukung, lihat Jenis Sumber Daya yang Didukung.

1. Gunakan `put-configuration-recorder`perintah:

   Perintah ini menggunakan `--configuration-recorder` dan `---recording-group` bidang.

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

`configuration-recorder`Bidang

`configurationRecorder.json`File menentukan `name` dan `roleArn` serta frekuensi perekaman default untuk perekam konfigurasi (`recordingMode`).

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

`recording-group`Bidang

`recordingGroup.json`File menentukan jenis sumber daya yang AWS Config akan merekam. Lulus satu atau beberapa jenis sumber daya untuk dikecualikan di `resourceTypes` bidang`exclusionByResourceTypes`, seperti yang ditunjukkan pada contoh berikut.

```
{
    "allSupported": false,
    "exclusionByResourceTypes": {
        "resourceTypes": [
            "AWS::Redshift::ClusterSnapshot",
            "AWS::RDS::DBClusterSnapshot",
            "AWS::CloudFront::StreamingDistribution"
        ]
    },
```

```
    "includeGlobalResourceTypes": false,
    "recordingStrategy": {
        "useOnly": "EXCLUSION_BY_RESOURCE_TYPES"
     },

}
```

Untuk informasi selengkapnya tentang bidang ini, lihat put-configuration-recorderdi Referensi AWS CLI Perintah.

2. (Opsional) Untuk memverifikasi bahwa perekam konfigurasi terkelola pelanggan Anda memiliki pengaturan yang Anda inginkan, gunakan describe-configuration-recordersperintah berikut.

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

Berikut ini adalah contoh respons.

```
{
    "ConfigurationRecorders": [
        {
            "name": "default",
            "recordingGroup": {
                "allSupported": false,
                "exclusionByResourceTypes": {
                    "resourceTypes": [
                        "AWS::Redshift::ClusterSnapshot",
                        "AWS::RDS::DBClusterSnapshot",
                        "AWS::CloudFront::StreamingDistribution"
                    ]
                },
                "includeGlobalResourceTypes": false,
                "recordingStrategy": {
                    "useOnly": "EXCLUSION_BY_RESOURCE_TYPES"
                },
                "resourceTypes": [],
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
```

```
                    "recordingFrequency": CONTINUOUS or DAILY,
                    "resourceTypes": [ Comma-separated list of resource types to
 include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

Record specific resource types

Siapkan AWS Config untuk merekam perubahan konfigurasi hanya untuk jenis sumber daya yang Anda tentukan.

Jika Anda memilih untuk berhenti merekam untuk jenis sumber daya, item konfigurasi yang sudah direkam akan tetap tidak berubah. Untuk daftar jenis sumber daya yang didukung, lihat Jenis Sumber Daya yang Didukung.

1. Gunakan `put-configuration-recorder`perintah:

   Perintah ini menggunakan `--configuration-recorder` dan `---recording-group` bidang.

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

   `configuration-recorder`Bidang

   `configurationRecorder.json`File menentukan `name` dan `roleArn` serta frekuensi perekaman default untuk perekam konfigurasi (`recordingMode`).

   ```
   {
     "name": "default",
     "roleARN": "arn:aws:iam::123456789012:role/config-role",
     "recordingMode": {
       "recordingFrequency": CONTINUOUS or DAILY,
       "recordingModeOverrides": [
           {
   ```

```
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include
 in the override ]
        }
    ]
  }
}
```

`recording-group`Bidang

`recordingGroup.json`File menentukan jenis sumber daya yang AWS Config akan merekam. Berikan satu atau beberapa jenis sumber daya untuk dikecualikan di `resourceTypes` bidang seperti yang ditunjukkan pada contoh berikut.

```
{
    "allSupported": false,
    "recordingStrategy": {
        "useOnly": "INCLUSION_BY_RESOURCE_TYPES"
    },
    "includeGlobalResourceTypes": false,
    "resourceTypes": [
        "AWS::EC2::EIP",
        "AWS::EC2::Instance",
        "AWS::EC2::NetworkAcl",
        "AWS::EC2::SecurityGroup",
        "AWS::CloudTrail::Trail",
        "AWS::EC2::Volume",
        "AWS::EC2::VPC",
        "AWS::IAM::User",
        "AWS::IAM::Policy"
  ]
}
```

Untuk informasi selengkapnya tentang bidang ini, lihat `put-configuration-recorder`di Referensi AWS CLI Perintah.

2. (Opsional) Untuk memverifikasi bahwa perekam konfigurasi terkelola pelanggan Anda memiliki pengaturan yang Anda inginkan, gunakan `describe-configuration-recorders`perintah berikut.

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

Berikut ini adalah contoh respons.

```
{
    "ConfigurationRecorders": [
        {
            "name": "default",
            "recordingGroup": {
                "allSupported": false,
                "exclusionByResourceTypes": {
                    "resourceTypes": []
                },
                "includeGlobalResourceTypes": false
                "recordingStrategy": {
                    "useOnly": "INCLUSION_BY_RESOURCE_TYPES"
                },
                "resourceTypes": [
                    "AWS::EC2::EIP",
                    "AWS::EC2::Instance",
                    "AWS::EC2::NetworkAcl",
                    "AWS::EC2::SecurityGroup",
                    "AWS::CloudTrail::Trail",
                    "AWS::EC2::Volume",
                    "AWS::EC2::VPC",
                    "AWS::IAM::User",
                    "AWS::IAM::Policy"
                ]
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types to
 include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
```

```
    ]
}
```

Mengecualikan sumber daya dari perekaman dengan AWS Config

AWS Config memungkinkan Anda untuk mengecualikan jenis AWS sumber daya tertentu dari pelacakan inventaris dan pemantauan kepatuhan sambil tetap melacak semua jenis sumber daya lain yang didukung saat ini tersedia AWS Config, termasuk yang akan ditambahkan di masa mendatang. Anda dapat menggunakan fitur ini untuk berkonsentrasi pada sumber daya penting yang tunduk pada standar kepatuhan dan tata kelola Anda.

Excluding resources (Console)

Jika Anda tidak ingin merekam jenis AWS sumber daya, gunakan salah satu strategi perekaman berikut untuk AWS Config konsol:

- Rekam semua jenis sumber daya dengan penggantian yang dapat disesuaikan, pilih jenis sumber daya yang ingin Anda kecualikan, dan pilih penggantian “Kecualikan dari perekaman”
- Rekam jenis sumber daya tertentu.

Untuk langkah selengkapnya, lihat Merekam sumber daya (Konsol).

Excluding resources (AWS CLI)

Jika Anda tidak ingin merekam jenis AWS sumber daya, gunakan salah satu strategi perekaman berikut untuk API/CLI:

- Rekam semua jenis sumber daya saat ini dan masa depan dengan pengecualian () `EXCLUSION_BY_RESOURCE_TYPES`
- Rekam jenis sumber daya tertentu (`INCLUSION_BY_RESOURCE_TYPES`).

Untuk langkah selengkapnya, lihat Merekam Sumber Daya (AWS CLI).

AWS Config Berhenti merekam dengan perekam konfigurasi terkelola pelanggan

Anda dapat berhenti AWS Config merekam dengan perekam konfigurasi yang dikelola pelanggan kapan saja. Setelah AWS Config berhenti merekam sumber daya, ia mempertahankan informasi konfigurasi yang sebelumnya ditangkap, dan Anda dapat terus mengakses informasi ini.

Untuk langkah-langkah tentang cara menghentikan perekaman, lihat Menghentikan perekam konfigurasi terkelola pelanggan.

Merekam Konfigurasi dengan AWS Config Sumber Daya Pihak Ketiga menggunakan AWS CLI

Rekam konfigurasi untuk sumber daya pihak ketiga atau jenis sumber daya khusus seperti pada server premis, alat pemantauan SAAS, dan sistem kontrol versi (seperti). GitHub

Anda dapat mempublikasikan data konfigurasi sumber daya pihak ketiga ke dalam AWS Config dan melihat serta memantau inventaris sumber daya dan riwayat konfigurasi menggunakan AWS Config konsol dan APIs. Anda dapat menggunakan AWS Config untuk mengelola semua sumber daya Anda dan mengevaluasi konfigurasi sumber daya untuk kepatuhan terhadap praktik terbaik menggunakan AWS Config aturan. Anda juga dapat membuat AWS Config aturan atau paket kesesuaian untuk mengevaluasi sumber daya pihak ketiga ini terhadap praktik terbaik, kebijakan internal, dan kebijakan peraturan.

> **Note**
>
> Jika Anda telah mengonfigurasi AWS Config untuk merekam semua jenis sumber daya, maka sumber daya pihak ketiga yang dikelola (dibuat, diperbarui, atau dihapus) secara otomatis AWS CloudFormation dilacak AWS Config sebagai item konfigurasi.

Prasyarat: Sumber daya pihak ketiga atau jenis sumber daya khusus harus didaftarkan menggunakan. AWS CloudFormation

Topik

- Menambahkan Sumber Daya Pihak Ketiga ke AWS Config
- Rekam Item Konfigurasi dengan AWS Config Sumber Daya Pihak Ketiga menggunakan AWS CLI

- Baca Item Konfigurasi dengan AWS Config Sumber Daya Pihak Ketiga menggunakan AWS CLI
- Hapus Sumber Daya Pihak Ketiga dari AWS Config menggunakan AWS CLI

Menambahkan Sumber Daya Pihak Ketiga ke AWS Config

Ikuti langkah-langkah ini untuk menambahkan sumber daya pihak ketiga AWS Config.

Topik

- Langkah 1: Siapkan Lingkungan Pengembangan Anda
- Langkah 2: Modelkan Sumber Daya Anda
- Langkah 3: Hasilkan Artefak
- Langkah 4: Daftarkan Sumber Daya Anda
- Langkah 5: Publikasikan Konfigurasi Sumber Daya

Langkah 1: Siapkan Lingkungan Pengembangan Anda

Instal dan konfigurasikan AWS CloudFormation AWS CLI. AWS CLI Ini memungkinkan Anda untuk memodelkan dan mendaftarkan sumber daya khusus Anda. Untuk informasi selengkapnya, lihat Sumber Daya Kustom dan Apa itu Antarmuka Baris CloudFormation Perintah? .

Langkah 2: Modelkan Sumber Daya Anda

Buat skema penyedia sumber daya yang sesuai dengan dan memvalidasi konfigurasi jenis sumber daya.

1. Gunakan `init` perintah untuk membuat proyek penyedia sumber daya Anda dan menghasilkan file yang dibutuhkan.

   ```
   $ cfn init
   Initializing new project
   ```

2. `init`Perintah meluncurkan wizard yang memandu Anda melalui pengaturan proyek, termasuk menentukan nama sumber daya. Untuk panduan ini, tentukan. `MyCustomNamespace::Testing::WordPress`

   ```
   Enter resource type identifier (Organization::Service::Resource):
    MyCustomNamespace::Testing::WordPress
   ```

3. Masukkan nama paket untuk sumber daya Anda.

```
Enter a package name (empty for default 'com.custom.testing.wordpress'):
 com.custom.testing.wordpress
Initialized a new project in /workplace/user/custom-testing-wordpress
```

> **Note**
>
> Untuk menjamin bahwa setiap dependensi proyek diselesaikan dengan benar, Anda dapat mengimpor proyek yang dihasilkan ke IDE Anda dengan dukungan Maven. Misalnya, jika Anda menggunakan IntelliJ IDEA, Anda perlu melakukan hal berikut:
>
> - Dari menu File, pilih New, lalu pilih Project From Existing Sources.
> - Arahkan ke direktori proyek
> - Dalam kotak dialog Impor Proyek, pilih Impor proyek dari model eksternal dan kemudian pilih Maven.
> - Pilih Berikutnya dan terima default apa pun untuk menyelesaikan pengimporan proyek.

4. Buka `mycustomnamespace-testing-wordpress.json` file yang berisi skema untuk sumber daya Anda. Salin dan tempel skema berikut ke dalam`mycustomnamespace-testing-wordpress.json`.

```
{
  "typeName": "MyCustomNamespace::Testing::WordPress",
  "description": "An example resource that creates a website based on WordPress
 5.2.2.",
  "properties": {
    "Name": {
      "description": "A name associated with the website.",
      "type": "string",
      "pattern": "^[a-zA-Z0-9]{1,219}\\Z",
      "minLength": 1, "maxLength": 219
    },
    "SubnetId": {
      "description": "A subnet in which to host the website.",
      "pattern": "^(subnet-[a-f0-9]{13})|(subnet-[a-f0-9]{8})\\Z",
      "type": "string"
    },
    "InstanceId": {
      "description": "The ID of the instance that backs the WordPress site.",
```

```
      "type": "string"
    },
    "PublicIp": {
      "description": "The public IP for the WordPress site.",
      "type": "string"
    }
  },
  "required": [ "Name", "SubnetId" ],
  "primaryIdentifier": [ "/properties/PublicIp", "/properties/InstanceId" ],
  "readOnlyProperties": [ "/properties/PublicIp", "/properties/InstanceId" ],
  "additionalProperties": false
}
```

5. Validasi skema.

```
$ cfn validate
```

6. Perbarui file yang dibuat secara otomatis dalam paket penyedia sumber daya untuk melihat pembaruan skema penyedia sumber daya. Setelah memulai proyek penyedia sumber daya, AWS CLI menghasilkan file pendukung dan kode untuk penyedia sumber daya. Regenerasi kode untuk melihat skema yang diperbarui.

```
$ cfn generate
```

> **Note**
>
> Saat menggunakan Maven, sebagai bagian dari proses build, `generate` perintah dijalankan secara otomatis sebelum kode dikompilasi. Jadi perubahan Anda tidak akan pernah keluar dari sinkron dengan kode yang dihasilkan.
> Sadarilah CloudFormation CLI harus berada di lokasi MAVEN/sistem dapat menemukan. Untuk informasi selengkapnya, lihat Menyiapkan lingkungan untuk mengembangkan ekstensi.

Untuk informasi selengkapnya tentang keseluruhan proses, lihat Pemodelan Penyedia Sumber Daya untuk Digunakan di AWS CloudFormation.

Langkah 3: Hasilkan Artefak

Jalankan perintah berikut untuk menghasilkan artefak untuk`cfn submit`.

```
$ mvn package
```

Langkah 4: Daftarkan Sumber Daya Anda

AWS Config tidak memerlukan penangan penyedia sumber daya untuk melakukan pelacakan konfigurasi untuk sumber daya Anda. Jalankan perintah berikut untuk mendaftarkan sumber daya Anda.

```
$ cfn submit
```

Untuk informasi selengkapnya, lihat Mendaftarkan Penyedia Sumber Daya untuk Digunakan di AWS CloudFormation Templat.

Langkah 5: Publikasikan Konfigurasi Sumber Daya

Tentukan konfigurasi untuk MyCustomNamespace: :Testing::WordPress.

```
{
  "Name": "MyWordPressSite",
  "SubnetId": "subnet-abcd0123",
  "InstanceId": "i-01234567",
  "PublicIp": "my-wordpress-site.com"
}
```

Tentukan id versi skema dari AWS CloudFormation `DescribeType`.

Di AWS Config, Anda dapat melihat apakah konfigurasi sumber daya ini diterima. Untuk mengevaluasi kepatuhan, Anda dapat menulis AWS Config aturan menggunakan sumber daya ini.

(Opsional) Untuk mengotomatiskan perekaman konfigurasi, terapkan kolektor konfigurasi periodik atau berbasis perubahan.

Rekam Item Konfigurasi dengan AWS Config Sumber Daya Pihak Ketiga menggunakan AWS CLI

Merekam item konfigurasi untuk sumber daya pihak ketiga atau jenis sumber daya khusus menggunakan prosedur berikut:

Pastikan Anda mendaftarkan jenis sumber daya `MyCustomNamespace::Testing::WordPress` dengan skema pencocokannya.

1. Buka jendela command prompt atau terminal.
2. Masukkan perintah berikut:

```
aws configservice put-resource-config --resource-type
 MyCustomNamespace::Testing::WordPress --resource-id resource-001 --schema-version-
id 00000001 --configuration  '{
  "Id": "resource-001",
  "Name": "My example custom resource.",
  "PublicAccess": false
}'
```

> **Note**
>
> Seperti yang didefinisikan dalam skema tipe, `writeOnlyProperties` akan dihapus dari konfigurasi sebelum direkam oleh AWS Config. Ini berarti bahwa nilai-nilai ini tidak akan ada ketika konfigurasi diperoleh dari baca APIs. Untuk informasi selengkapnya`writeOnlyProperties`, lihat Skema tipe sumber daya.

Baca Item Konfigurasi dengan AWS Config Sumber Daya Pihak Ketiga menggunakan AWS CLI

Membaca item konfigurasi untuk sumber daya pihak ketiga atau jenis sumber daya khusus menggunakan prosedur berikut:

1. Buka jendela command prompt atau terminal.
2. Masukkan perintah berikut:

```
aws configservice list-discovered-resources --resource-type
 MyCustomNamespace::Testing::WordPress
```

3. Tekan Enter.

   Anda akan melihat output yang serupa dengan yang berikut:

```
{
    "resourceIdentifiers": [
        {
```

```
            "resourceType": "MyCustomNamespace::Testing::WordPress",
            "resourceId": "resource-001"
        }
    ]
}
```

4. Masukkan perintah berikut:

```
aws configservice batch-get-resource-config --resource-keys '[ { "resourceType":
 "MyCustomNamespace::Testing::WordPress", "resourceId": "resource-001" } ]'
```

5. Tekan Enter.

   Anda akan melihat output yang serupa dengan yang berikut:

```
{
    "unprocessedResourceKeys": [],
    "baseConfigurationItems": [
        {
            "configurationItemCaptureTime": 1569605832.673,
            "resourceType": "MyCustomNamespace::Testing::WordPress",
            "resourceId": "resource-001",
            "configurationStateId": "1569605832673",
            "awsRegion": "us-west-2",
            "version": "1.3",
            "supplementaryConfiguration": {},
            "configuration": "{\"Id\":\"resource-001\",\"Name\":\"My example custom
 resource.\",\"PublicAccess\":false}",
            "configurationItemStatus": "ResourceDiscovered",
            "accountId": "AccountId"
        }
    ]
}
```

Hapus Sumber Daya Pihak Ketiga dari AWS Config menggunakan AWS CLI

Masukkan perintah berikut untuk menghapus sumber daya pihak ketiga:

```
aws configservice delete-resource-config --resource-type
 MyCustomNamespace::Testing::WordPress --resource-id resource-002
```

Jika berhasil, perintah dijalankan tanpa output tambahan.

Merekam Konfigurasi Perangkat Lunak untuk Instans Terkelola dengan AWS Config

Anda dapat menggunakan AWS Config untuk merekam perubahan inventaris perangkat lunak di EC2 instans Amazon dan server lokal. Ini memungkinkan Anda untuk melihat perubahan historis pada konfigurasi perangkat lunak. Misalnya, ketika pembaruan Windows baru diinstal pada instance Windows yang dikelola, AWS Config catat perubahan dan kemudian mengirimkan perubahan ke saluran pengiriman Anda, sehingga Anda diberi tahu tentang perubahan tersebut. Dengan AWS Config, Anda dapat melihat riwayat kapan pembaruan Windows diinstal untuk instance terkelola dan bagaimana mereka berubah dari waktu ke waktu.

Topik

- Prasyarat
- Konfigurasi Perangkat Lunak Perekaman

Prasyarat

Anda harus menyelesaikan langkah-langkah berikut untuk merekam perubahan konfigurasi perangkat lunak:

- Aktifkan perekaman untuk tipe sumber daya inventaris instans terkelola AWS Config.
- Mengkonfigurasi EC2 dan server lokal sebagai instance terkelola di. AWS Systems Manager Sebuah instance terkelola adalah mesin yang telah dikonfigurasi untuk digunakan dengan Systems Manager.
- Memulai pengumpulan inventaris perangkat lunak dari instans terkelola Anda menggunakan kemampuan Systems Manager Inventory.

> **Note**
>
> Systems Manager sekarang mendukung pembuatan item konfigurasi untuk instance yang tidak dikelola

Item konfigurasi untuk instance yang tidak dikelola akan memiliki konfigurasi tambahan dengan dan. `Key: “InstanceStatus”` `Value: “Unmanaged”`
Item konfigurasi untuk instans yang tidak dikelola tidak akan menerima pembaruan tambahan
Untuk menerima pembaruan tambahan, item konfigurasi harus berupa instance terkelola.

Anda juga dapat menggunakan AWS Config aturan untuk memantau perubahan konfigurasi perangkat lunak dan diberi tahu apakah perubahan tersebut sesuai atau tidak sesuai dengan aturan Anda. Misalnya, jika Anda membuat aturan yang memeriksa apakah instance terkelola Anda memiliki aplikasi tertentu, dan instans tidak menginstal aplikasi tersebut, AWS Config menandai instance tersebut sebagai tidak sesuai dengan aturan Anda. Untuk daftar aturan AWS Config terkelola, lihatDaftar Aturan AWS Config Terkelola.

Konfigurasi Perangkat Lunak Perekaman

Untuk mengaktifkan perekaman perubahan konfigurasi perangkat lunak di AWS Config:

1. Aktifkan perekaman untuk semua jenis sumber daya yang didukung atau rekam secara selektif jenis sumber daya inventaris instans terkelola. AWS Config Untuk informasi selengkapnya, lihat Merekam AWS Sumber Daya dengan AWS Config.
2. Luncurkan EC2 instans Amazon dengan profil instans untuk Systems Manager yang menyertakan kebijakan SSMManaged InstanceCore terkelola Amazon. Kebijakan AWS terkelola ini memungkinkan instans untuk menggunakan fungsi inti layanan Systems Manager.

   Untuk informasi tentang kebijakan lain yang dapat Anda tambahkan ke profil instans untuk Systems Manager, lihat Membuat Profil Instans IAM untuk Systems Manager di Panduan AWS Systems Manager Pengguna.

   Important

   SSM Agent adalah perangkat lunak Amazon yang harus diinstal pada instance terkelola untuk berkomunikasi dengan Systems Manager di cloud. Jika EC2 instans Anda dibuat dari AMI untuk salah satu sistem operasi berikut, agen sudah diinstal sebelumnya:

   - Windows Server 2003-2012 R2 AMIs diterbitkan pada November 2016 atau lebih baru
   - Windows Server 2016 dan 2019
   - Amazon Linux

- Amazon Linux 2
- Server Ubuntu 16.04
- Server Ubuntu 18.04

Pada EC2 instance yang tidak dibuat dari AMI dengan agen yang sudah diinstal sebelumnya, Anda harus menginstal agen secara manual. Untuk selengkapnya, lihat topik berikut di Panduan AWS Systems Manager Pengguna:

- Menginstal dan mengonfigurasi Agen SSM pada EC2 instance untuk Windows Server
- Menginstal dan mengonfigurasi Agen SSM pada EC2 instance untuk Linux

3. Memulai pengumpulan inventaris seperti yang dijelaskan dalam Mengonfigurasi Koleksi Inventaris di AWS Systems Manager Panduan Pengguna. Prosedurnya sama untuk instance Linux dan Windows.

   AWS Config dapat merekam perubahan konfigurasi untuk jenis inventaris berikut:

   - Aplikasi — Daftar aplikasi untuk instance terkelola, seperti perangkat lunak antivirus.
   - AWS komponen — Daftar AWS komponen untuk instance terkelola, seperti AWS CLI dan SDKs.
   - Informasi instans — Informasi instans seperti nama dan versi OS, domain, dan status firewall.
   - Konfigurasi jaringan — Informasi konfigurasi seperti alamat IP, gateway, dan subnet mask.
   - Pembaruan Windows — Daftar pembaruan Windows untuk instance terkelola (hanya instance Windows).

   > **Note**
   >
   > AWS Config tidak mendukung perekaman jenis inventaris khusus saat ini.

Pengumpulan inventaris adalah salah satu dari banyak kemampuan Systems Manager, yang dikelompokkan dalam kategori Operations Management, Actions & Change, Instances & Nodes, dan Shared Resources. Untuk informasi selengkapnya, lihat Apa itu Systems Manager? dan Kemampuan Systems Manager di Panduan AWS Systems Manager Pengguna.

Mencari Sumber Daya yang Ditemukan oleh AWS Config

Anda dapat menggunakan AWS Config konsol, AWS CLI, dan AWS Config API untuk mencari sumber daya yang AWS Config telah mengambil inventarisasi, atau ditemukan, termasuk sumber daya yang dihapus dan sumber daya yang saat AWS Config ini tidak direkam. AWS Config menemukan jenis sumber daya yang didukung saja. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.

Looking Up Resources (Console)

Anda dapat menggunakan jenis sumber daya atau informasi tag untuk mencari sumber daya di AWS Config konsol.

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Pada halaman Inventaris sumber daya, tentukan opsi pencarian untuk sumber daya yang ingin Anda cari:
   - Kategori sumber daya — Pilih semua kategori sumber daya atau persempit hasil hanya AWS Sumber Daya.
   - Jenis sumber daya - Pilih semua jenis sumber daya atau pilih sumber daya mana yang akan difilter.
   - Kepatuhan — Pilih untuk memfilter berdasarkan status kepatuhan, patuh, atau tidak patuh.
3. AWS Config daftar sumber daya yang cocok dengan opsi pencarian Anda. Anda dapat melihat informasi berikut tentang sumber daya:
   - Pengenal sumber daya — Pengidentifikasi sumber daya mungkin berupa ID sumber daya atau nama sumber daya, jika berlaku. Pilih tautan pengenal sumber daya untuk melihat halaman detail sumber daya.
   - Jenis sumber daya — Jenis sumber daya terdaftar.
   - Kepatuhan — Status sumber daya yang AWS Config dievaluasi terhadap aturan Anda.

Looking Up Resources (AWS CLI)

Anda dapat menggunakan daftar sumber daya yang AWS Config telah ditemukan. AWS CLI

Gunakan AWS Config service `list-discovered-resources` perintah:

```
$ aws configservice list-discovered-resources --resource-type "AWS::EC2::Instance"
        {
            "resourceIdentifiers": [
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-nnnnnnnn"
                }
            ]
        }
```

Untuk melihat detail konfigurasi sumber daya yang tercantum dalam respons, gunakan `get-resource-config-history`perintah, dan tentukan jenis sumber daya dan ID. Untuk contoh perintah ini dan tanggapan dari AWS Config, lihatMelihat Riwayat Konfigurasi.

Looking up Resources (API)

Anda menentukan jenis sumber daya, dan AWS Config mengembalikan daftar pengidentifikasi sumber daya untuk sumber daya jenis tersebut. Untuk informasi selengkapnya, lihat ResourceIdentifier di dalam Referensi API AWS Config .

Gunakan ListDiscoveredResourcestindakan.

Untuk mendapatkan detail konfigurasi sumber daya yang tercantum dalam respons, gunakan GetResourceConfigHistorytindakan, dan tentukan jenis dan ID sumber daya.

Melihat Informasi Kepatuhan dan Hasil Evaluasi untuk AWS Sumber Daya Anda dengan AWS Config

> **Important**
>
> Untuk pelaporan yang akurat tentang status kepatuhan, Anda harus mencatat jenis `AWS::Config::ResourceCompliance` sumber daya. Untuk informasi selengkapnya, lihat Merekam AWS Sumber Daya.

Anda dapat menggunakan AWS Config konsol atau AWS SDKs untuk melihat informasi kepatuhan dan hasil evaluasi sumber daya Anda.

Topik

- Melihat kepatuhan (Konsol)
- Melihat kepatuhan (AWS SDKs)

Melihat kepatuhan (Konsol)

Untuk melihat kepatuhan (Konsol)

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Di AWS Management Console menu, verifikasi bahwa pemilih wilayah diatur ke wilayah yang mendukung AWS Config aturan. Untuk daftar wilayah yang didukung, lihat AWS Config Wilayah dan Titik Akhir di. Referensi Umum Amazon Web Services
3. Pada panel navigasi, silakan pilih Sumber Daya. Pada halaman Inventaris sumber daya, Anda dapat memfilter berdasarkan kategori sumber daya, jenis sumber daya, dan status kepatuhan. Pilih Sertakan sumber daya yang dihapus jika sesuai. Tabel menampilkan pengenal sumber daya untuk jenis sumber daya dan status kepatuhan sumber daya untuk sumber daya tersebut. Pengidentifikasi sumber daya mungkin berupa ID sumber daya atau nama sumber daya.
4. Pilih sumber daya dari kolom pengenal sumber daya.
5. Pilih tombol Resource Timeline. Anda dapat memfilter berdasarkan peristiwa Konfigurasi, peristiwa Kepatuhan, atau CloudTrail Acara.

> **Note**
>
> Atau, pada halaman inventaris Sumber Daya, Anda dapat langsung memilih nama sumber daya. Untuk mengakses timeline sumber daya dari halaman detail sumber daya, pilih tombol Garis Waktu Sumber Daya.

Anda juga dapat melihat kepatuhan sumber daya Anda dengan mencarinya di halaman inventaris Sumber Daya. Untuk informasi selengkapnya, lihat Mencari Sumber Daya yang Ditemukan oleh AWS Config.

Melihat kepatuhan (AWS SDKs)

Untuk mendapatkan informasi kepatuhan untuk AWS sumber daya Anda

Contoh kode berikut menunjukkan cara menggunakan`DescribeComplianceByResource`.

CLI

AWS CLI

Untuk mendapatkan informasi kepatuhan untuk AWS sumber daya Anda

Perintah berikut mengembalikan informasi kepatuhan untuk setiap EC2 instance yang direkam oleh AWS Config dan yang melanggar satu atau beberapa aturan:

```
aws configservice describe-compliance-by-resource --resource-
type AWS::EC2::Instance --compliance-types NON_COMPLIANT
```

Dalam output, nilai untuk setiap `CappedCount` atribut menunjukkan berapa banyak aturan yang dilanggar sumber daya. Misalnya, output berikut menunjukkan bahwa instance `i-1a2b3c4d` melanggar 2 aturan.

Output:

```
{
    "ComplianceByResources": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-1a2b3c4d",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 2,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-2a2b3c4d ",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        }
    ]
```

```
}
```

- Untuk detail API, lihat DescribeComplianceByResourcedi Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Contoh ini memeriksa jenis **`AWS::SSM::ManagedInstanceInventory`** sumber daya untuk jenis kepatuhan 'COMPLIANT'.

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

Output:

```
Compliance                              ResourceId          ResourceType
----------                              ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- Untuk detail API, lihat DescribeComplianceByResourcedi Referensi Alat AWS untuk PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Contoh ini memeriksa jenis **`AWS::SSM::ManagedInstanceInventory`** sumber daya untuk jenis kepatuhan 'COMPLIANT'.

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

Output:

```
Compliance                              ResourceId          ResourceType
----------                              ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
```

```
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- Untuk detail API, lihat DescribeComplianceByResourcedi Referensi Alat AWS untuk PowerShell Cmdlet (V5).

Untuk mendapatkan ringkasan kepatuhan AWS sumber daya Anda

Contoh kode berikut menunjukkan cara menggunakan`GetComplianceSummaryByResourceType`.

CLI

AWS CLI

Untuk mendapatkan ringkasan kepatuhan untuk semua jenis sumber daya

Perintah berikut mengembalikan jumlah AWS sumber daya yang tidak sesuai dan nomor yang sesuai:

```
aws configservice get-compliance-summary-by-resource-type
```

Dalam output, nilai untuk setiap `CappedCount` atribut menunjukkan berapa banyak sumber daya yang sesuai atau tidak sesuai.

Output:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 16,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1453237464.543,
                "CompliantResourceCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                }
            }
        }
```

```
    ]
}
```

Untuk mendapatkan ringkasan kepatuhan untuk jenis sumber daya tertentu

Perintah berikut mengembalikan jumlah EC2 instance yang tidak sesuai dan nomor yang sesuai:

```
aws configservice get-compliance-summary-by-resource-type --resource-
types AWS::EC2::Instance
```

Dalam output, nilai untuk setiap `CappedCount` atribut menunjukkan berapa banyak sumber daya yang sesuai atau tidak sesuai.

Output:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1452204923.518,
                "CompliantResourceCount": {
                    "CappedCount": 7,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

- Untuk detail API, lihat GetComplianceSummaryByResourceTypedi Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Sampel ini mengembalikan jumlah sumber daya yang sesuai atau tidak sesuai dan mengubah output menjadi json.

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- Untuk detail API, lihat GetComplianceSummaryByResourceTypedi Referensi Alat AWS untuk PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Sampel ini mengembalikan jumlah sumber daya yang sesuai atau tidak sesuai dan mengubah output menjadi json.

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- Untuk detail API, lihat GetComplianceSummaryByResourceTypedi Referensi Alat AWS untuk PowerShell Cmdlet (V5).

Untuk mendapatkan hasil evaluasi untuk sumber AWS daya

Contoh kode berikut menunjukkan cara menggunakan`GetComplianceDetailsByResource`.

CLI

AWS CLI

Untuk mendapatkan hasil evaluasi untuk sumber AWS daya

Perintah berikut mengembalikan hasil evaluasi untuk setiap aturan yang EC2 instans `i-1a2b3c4d` tidak mematuhi:

```
aws configservice get-compliance-details-by-resource --resource-
type AWS::EC2::Instance --resource-id i-1a2b3c4d --compliance-types NON_COMPLIANT
```

Output:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.288,
            "ConfigRuleInvokedTime": 1450314643.034,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
```

```
                    "ConfigRuleName": "RequiredTagForEC2Instances"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- Untuk detail API, lihat GetComplianceDetailsByResourcedi Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Contoh evaulasi ini menghasilkan sumber daya yang diberikan.

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

Output:

```
Annotation                 :
ComplianceType             : COMPLIANT
ConfigRuleInvokedTime      : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime         : 8/25/2019 11:34:56 PM
ResultToken                :
```

- Untuk detail API, lihat GetComplianceDetailsByResourcedi Referensi Alat AWS untuk PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Contoh evaulasi ini menghasilkan sumber daya yang diberikan.

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

Output:

```
Annotation                  :
ComplianceType              : COMPLIANT
ConfigRuleInvokedTime       : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime          : 8/25/2019 11:34:56 PM
ResultToken                 :
```

- Untuk detail API, lihat GetComplianceDetailsByResourcedi Referensi Alat AWS untuk PowerShell Cmdlet (V5).

Melihat Riwayat Kepatuhan untuk AWS Sumber Daya Anda dengan AWS Config

> **Important**
>
> Jenis `AWS::Config::ResourceCompliance` sumber daya digunakan untuk menyimpan hasil kepatuhan historis untuk sumber daya. Merekam jenis sumber daya ini tidak diperlukan untuk aturan Config untuk mengevaluasi sumber daya atau untuk melihat status kepatuhan saat ini di konsol.
> Rekaman `AWS::Config::ResourceCompliance` hanya memungkinkan Anda untuk melihat perubahan kepatuhan historis dari waktu ke waktu di timeline sumber daya. Jika Anda tidak memerlukan data kepatuhan historis, Anda dapat mengecualikan jenis sumber daya ini. Untuk informasi selengkapnya tentang memilih sumber daya untuk direkam, lihat Merekam AWS Sumber Daya.

Anda dapat melihat konfigurasi, hubungan, dan jumlah perubahan yang dilakukan pada sumber daya di AWS Config konsol. Anda dapat melihat riwayat konfigurasi untuk sumber daya yang digunakan AWS CLI.

Topik

- Melihat Riwayat Kepatuhan (Konsol)
- Melihat Riwayat Kepatuhan (AWS CLI)
- Melihat Garis Waktu Riwayat Kepatuhan untuk Sumber Daya dan Aturan

Melihat Riwayat Kepatuhan (Konsol)

Melihat Riwayat Kepatuhan Menggunakan Konsol

Saat Anda mencari sumber daya di halaman inventaris Sumber daya, pilih nama atau ID sumber daya di kolom pengenal sumber daya untuk melihat halaman detail sumber daya. Halaman detail memberikan informasi tentang konfigurasi, hubungan, dan jumlah perubahan yang dilakukan pada sumber daya tersebut.

Untuk mengakses timeline sumber daya dari halaman detail sumber daya, pilih tombol Garis Waktu Sumber Daya. Garis waktu Sumber Daya menangkap perubahan `ConfigurationItems` selama periode waktu untuk sumber daya tertentu. Anda dapat memfilter berdasarkan peristiwa Konfigurasi, peristiwa Kepatuhan, atau CloudTrail Acara.

Melihat Riwayat Kepatuhan (AWS CLI)

Melihat Riwayat Kepatuhan Menggunakan AWS CLI

Item konfigurasi yang AWS Config merekam dikirim ke saluran pengiriman yang ditentukan sesuai permintaan sebagai snapshot konfigurasi dan sebagai aliran konfigurasi. Anda dapat menggunakan AWS CLI untuk melihat riwayat item konfigurasi untuk setiap sumber daya.

Melihat Riwayat Konfigurasi

Masukkan `get-resource-config-history`perintah dan tentukan jenis sumber daya dan ID sumber daya, misalnya:

```
$ aws configservice get-resource-config-history --resource-type AWS::EC2::SecurityGroup
 --resource-id sg-6fbb3807
{
    "configurationItems": [
        {
            "configurationItemCaptureTime": 1414708529.9219999,
            "relationships": [
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-7a3b232a",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-8b6eb2ab",
```

```
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-c478efe5",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-e4cbe38d",
                    "relationshipName": "Is associated with Instance"
                }
            ],
            "availabilityZone": "Not Applicable",
            "tags": {},
            "resourceType": "AWS::EC2::SecurityGroup",
            "resourceId": "sg-6fbb3807",
            "configurationStateId": "1",
            "relatedEvents": [],
            "arn": "arn:aws:ec2:us-east-2:012345678912:security-group/default",
            "version": "1.0",
            "configurationItemMD5Hash": "860aa81fc3869e186b2ee00bc638a01a",
            "configuration": "{\"ownerId\":\"605053316265\",\"groupName\":\"default
\",\"groupId\":\"sg-6fbb3807\",\"description\":\"default group\",\"ipPermissions
\":[{\"ipProtocol\":\"tcp\",\"fromPort\":80,\"toPort\":80,\"userIdGroupPairs\":
[{\"userId\":\"amazon-elb\",\"groupName\":\"amazon-elb-sg\",\"groupId\":\"sg-843f59ed
\"}],\"ipRanges\":[\"0.0.0.0/0\"]},{\"ipProtocol\":\"tcp\",\"fromPort\":0,\"toPort
\":65535,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName\":\"default
\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"udp\",\"fromPort
\":0,\"toPort\":65535,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName
\":\"default\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"icmp
\",\"fromPort\":-1,\"toPort\":-1,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",
\"groupName\":\"default\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol
\":\"tcp\",\"fromPort\":1433,\"toPort\":1433,\"userIdGroupPairs\":[],\"ipRanges
\":[\"0.0.0.0/0\"]},{\"ipProtocol\":\"tcp\",\"fromPort\":3389,\"toPort\":3389,
\"userIdGroupPairs\":[],\"ipRanges\":[\"207.171.160.0/19\"]}],\"ipPermissionsEgress\":
[],\"vpcId\":null,\"tags\":[]}",
            "configurationItemStatus": "ResourceDiscovered",
            "accountId": "605053316265"
        }
    ],
    "nextToken":
     ..........
```

Untuk penjelasan rinci tentang bidang respons, lihat Components of a Configuration Item danJenis Sumber Daya yang Didukung untuk AWS Config.

Contoh Riwayat Konfigurasi Amazon EBS dari AWS Config

AWS Config menghasilkan satu set file yang masing-masing mewakili jenis sumber daya dan mencantumkan semua perubahan konfigurasi untuk sumber daya dari jenis AWS Config yang merekam. AWS Config mengekspor riwayat konfigurasi yang berpusat pada sumber daya ini sebagai objek di bucket Amazon S3 yang Anda tentukan saat mengaktifkan. AWS Config File riwayat konfigurasi untuk setiap jenis sumber daya berisi perubahan yang terdeteksi untuk sumber daya jenis tersebut sejak file riwayat terakhir dikirimkan. File riwayat biasanya dikirim setiap enam jam.

Berikut ini adalah contoh konten objek Amazon S3 yang menjelaskan riwayat konfigurasi semua volume Amazon Elastic Block Store di wilayah saat ini untuk Anda. Akun AWS Volume dalam akun ini termasuk `vol-ce676ccc` dan`vol-cia007c`. Volume `vol-ce676ccc` memiliki dua perubahan konfigurasi sejak file riwayat sebelumnya dikirimkan sementara volume `vol-cia007c` memiliki satu perubahan.

```
{
    "fileVersion": "1.0",
    "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
    "configurationItems": [
        {
            "snapshotVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
            "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
```

```
                "name": "Attached to Instance"
            }
        ],
        "configuration": {
            "volumeId": "vol-ce676ccc",
            "size": 1,
            "snapshotId": "",
            "availabilityZone": "us-west-2b",
            "state": "in-use",
            "createTime": "2014-02-27T21:43:53.0885+0000",
            "attachments": [
                {
                    "volumeId": "vol-ce676ccc",
                    "instanceId": "i-344c463d",
                    "device": "/dev/sdf",
                    "state": "attached",
                    "attachTime": "2014-03-07T23:46:28.0000+0000",
                    "deleteOnTermination": false
                }
            ],
            "tags": [
                {
                    "tagName": "environment",
                    "tagValue": "PROD"
                },
                {
                    "tagName": "name",
                    "tagValue": "DataVolume1"
                }
            ],
            "volumeType": "standard"
        }
    },
    {
        "configurationItemVersion": "1.0",
        "resourceId": "vol-ce676ccc",
        "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
        "accountId": "12345678910",
        "configurationItemCaptureTime": "2014-03-07T21:47:08.918Z",
        "configurationItemState": "3e660fdf-4e34-4f32-sseb-0ace5bf3d63a",
        "configurationItemStatus": "OK",
        "relatedEvents": [
            "06c12a39-eb35-11de-ae07-ad229edbb1e4",
            "c376e30d-71a2-4694-89b7-a5a04w292281"
```

```
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume1"
                    }
                ],
                "volumeType": "standard"
            }
        },
        {
            "configurationItemVersion": "1.0",
```

```
            "resourceId": "vol-cia007c",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-cia007c",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T20:47:08.918Z",
            "configurationItemState": "3e660fdf-4e34-4f88-sseb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adjhk8edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a67u292281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T20:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344e563d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-cia007c",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T20:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-cia007c",
                        "instanceId": "i-344e563d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
```

```
                        "tagName": "name",
                        "tagValue": "DataVolume2"
                    }
                ],
                "volumeType": "standard"
            }
        }
    ]
}
```

Melihat Garis Waktu Riwayat Kepatuhan untuk Sumber Daya dan Aturan

AWS Config mendukung penyimpanan perubahan status kepatuhan sumber daya sebagaimana dievaluasi oleh Aturan AWS Config. Riwayat kepatuhan sumber daya disajikan dalam bentuk garis waktu. Garis waktu menangkap perubahan `ConfigurationItems` selama periode waktu untuk sumber daya tertentu. Untuk informasi tentang konten`ConfigurationItem`, lihat ConfigurationItemdi Referensi AWS Config API.

Anda dapat memilih masuk atau keluar untuk merekam semua jenis sumber daya AWS Config. Jika Anda memilih untuk merekam semua jenis sumber daya, AWS Config secara otomatis mulai merekam riwayat kepatuhan sumber daya seperti yang dievaluasi oleh. Aturan AWS Config Secara default, AWS Config mencatat perubahan konfigurasi untuk semua sumber daya yang didukung. Anda juga dapat memilih hanya jenis sumber daya riwayat kepatuhan sumber daya tertentu:`AWS::Config::ResourceCompliance`. Untuk informasi selengkapnya, lihat Merekam AWS Rekaman.

Viewing Resource Timeline Using Resources

Akses timeline sumber daya dengan memilih sumber daya tertentu dari halaman inventaris Sumber Daya.

1. Pilih Sumber Daya dari navigasi kiri.
2. Pada halaman Inventaris sumber daya, Anda dapat memfilter berdasarkan kategori sumber daya, jenis sumber daya, dan status kepatuhan. Pilih Sertakan sumber daya yang dihapus jika sesuai.

   Tabel menampilkan pengenal sumber daya untuk jenis sumber daya dan status kepatuhan sumber daya untuk sumber daya tersebut. Pengidentifikasi sumber daya mungkin berupa ID sumber daya atau nama sumber daya.
3. Pilih sumber daya dari kolom pengenal sumber daya.

4. Pilih tombol Resource Timeline. Anda dapat memfilter berdasarkan peristiwa Konfigurasi, peristiwa Kepatuhan, atau CloudTrail Acara.

> **Note**
>
> Atau, pada halaman inventaris Sumber Daya, Anda dapat langsung memilih nama sumber daya. Untuk mengakses timeline sumber daya dari halaman detail sumber daya, pilih tombol Garis Waktu Sumber Daya.

Viewing Resource Timeline Using Rules

Akses timeline sumber daya dengan memilih aturan tertentu dari halaman Aturan.

1. Pilih Aturan dari navigasi kiri.
2. Pada halaman Aturan, pilih aturan yang mengevaluasi sumber daya Anda yang relevan. Jika tidak ada aturan yang ditampilkan di layar, tambahkan aturan menggunakan tombol Tambahkan aturan.
3. Pada halaman Rincian aturan, pilih sumber daya dari tabel Resources evaluated.
4. Pilih tombol Resource Timeline. Garis waktu sumber daya ditampilkan.

Menanyakan Riwayat Kepatuhan untuk Sumber Daya Anda AWS

Kueri riwayat kepatuhan sumber daya get-resource-config-history menggunakan jenis sumber daya`AWS::Config::ResourceCompliance`.

```
aws configservice get-resource-config-history --resource-type
 AWS::Config::ResourceCompliance --resource-id AWS::S3::Bucket/configrules-bucket
```

Anda akan melihat output yang serupa dengan yang berikut:

```
{
 "configurationItems": [
  {
   "configurationItemCaptureTime": 1539799966.921,
   "relationships": [
    {
     "resourceType": "AWS::S3::Bucket",
```

```
      "resourceId": "configrules-bucket",
      "relationshipName": "Is associated with "
     }
    ]
    "tags": {},
    "resourceType": "AWS::Config::ResourceCompliance",
    "resourceId": "AWS::S3::Bucket/configrules-bucket",
    "ConfigurationStateId": "1539799966921",
    "relatedEvents": [];
    "awsRegion": "us-west-2",
    "version": "1.3",
    "configurationItemMD5Hash": "",
    "supplementaryConfiguration": {},
    "configuration": "{\"complianceType\":\"COMPLIANT\",\"targetResourceId\":
\"configrules-bucket\",\"targetResourceType\":\"AWS::S3::Bucket\",\configRuleList"\":
[{\"configRuleArn\":\"arn:aws:config:us-west-2:AccountID:config-rule/config-rule-w1gogw
\",\"configRuleId\":\"config-rule-w1gogw\",\"configRuleName\":\"s3-bucket-logging-
enabled\",\"complianceType\":\"COMPLIANT\"}]}",

    "configurationItemStatus": "ResourceDiscovered",
    "accountId": "AccountID"
   }
  ]
}
```

Menandai Sumber Daya Anda AWS Config

Tag adalah label yang Anda tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci dan nilai opsional, yang keduanya Anda tentukan. Tag membuatnya lebih mudah untuk mengelola, mencari, dan memfilter sumber daya.

Tag memungkinkan Anda untuk mengkategorikan AWS sumber daya Anda dengan cara yang berbeda, misalnya, berdasarkan tujuan, pemilik, atau lingkungan. Hal ini berguna ketika Anda memiliki banyak sumber daya dengan jenis yang sama—Anda dapat dengan cepat mengidentifikasi sumber daya tertentu berdasarkan tanda yang telah Anda tetapkan. Anda dapat menetapkan satu atau beberapa tag ke AWS sumber daya Anda. Setiap tag memiliki nilai terkait.

Sebaiknya rancang serangkaian kunci tag yang memenuhi kebutuhan setiap jenis sumber daya. Menggunakan satu set kunci tag yang konsisten memudahkan Anda mengelola AWS sumber daya Anda. Anda dapat mencari dan memfilter sumber daya berdasarkan tag yang Anda tambahkan.

Tag ditafsirkan secara ketat sebagai serangkaian karakter dan tidak secara otomatis ditetapkan ke sumber daya Anda. Anda dapat mengedit kunci dan nilai tanda, dan dapat menghapus tanda dari sumber daya kapan saja. Anda dapat mengatur nilai tanda ke string kosong, tetapi tidak dapat mengatur nilai tanda ke null. Jika Anda menambahkan tanda yang memiliki kunci yang sama dengan tanda yang telah ada pada sumber daya tersebut, nilai yang baru akan menimpa nilai yang lama. Jika sumber daya dihapus, semua tanda untuk sumber daya tersebut juga akan dihapus.

Anda dapat bekerja dengan tag menggunakan AWS Command Line Interface (AWS CLI) dan referensi AWS Config API.

Pembatasan Terkait Penandaan

Pembatasan dasar berikut berlaku untuk tag.

Pembatasan	Deskripsi
Jumlah maksimum tanda per sumber daya	50
Panjang kueri maksimum	128 karakter Unicode dalam UTF-8
Panjang nilai maksimum	256 karakter Unicode dalam UTF-8
Pembatasan prefiks	Jangan gunakan `aws:` awalan dalam nama atau nilai tag Anda karena itu dicadangkan untuk AWS digunakan. Anda tidak dapat mengedit atau menghapus nama atau nilai tag dengan awalan ini. Tag dengan awalan ini tidak dihitung terhadap tag Anda per batas sumber daya.
Pembatasan karakter	Tanda hanya boleh berisi huruf Unicode, angka, spasi putih, atau simbol berikut: `_ . : / = + - @`.

Mengelola Tag dengan Tindakan AWS Config API

Kontrol akses berbasis tag tersedia untuk tiga sumber dayaConfigurationAggregator,AggregationAuthorization, danConfigRule. Gunakan

hal-hal berikut untuk menambahkan, memperbarui, mencantumkan, dan menghapus tanda untuk sumber daya Anda.

- ListTagsForResource
- TagResource
- UntagResource

> **Note**
>
> `TagResource`dan `UntagResource` memerlukan izin AWS Identity and Access Management (IAM) tertentu untuk mengontrol akses. Untuk informasi selengkapnya, lihat Mengontrol akses berdasarkan kunci tag di Panduan Pengguna IAM.

Mengevaluasi Sumber Daya dengan Aturan AWS Config

Gunakan AWS Config untuk mengevaluasi pengaturan konfigurasi AWS sumber daya Anda. Anda melakukan ini dengan membuat AWS Config aturan, yang mewakili pengaturan konfigurasi ideal Anda. AWS Config menyediakan aturan yang dapat disesuaikan dan telah ditentukan sebelumnya yang disebut aturan terkelola untuk membantu Anda memulai.

Topik

- Pertimbangan
- Support Wilayah
- Komponen AWS Config Aturan
- AWS Config Aturan yang Dikelola
- AWS Config Aturan Kustom
- Aturan Terkait Layanan AWS Config
- Mengelola AWS Config Aturan di Semua Akun di Organisasi Anda
- Menambahkan AWS Config Aturan
- Memperbarui AWS Config Aturan
- Menghapus Aturan AWS Config
- Melihat Detail dan Informasi Kepatuhan untuk AWS Config Aturan Anda
- Mengaktifkan Evaluasi Proaktif untuk Aturan AWS Config
- Mengirim Evaluasi Aturan ke Security Hub
- Mengevaluasi Sumber Daya Anda dengan Aturan AWS Config
- Menghapus Hasil Evaluasi dari Aturan AWS Config
- Pemecahan masalah untuk aturan AWS Config

Pertimbangan

Cost Considerations

Untuk detail tentang biaya yang terkait dengan pencatatan sumber daya, lihat AWS Config harga.

Rekomendasi: Pertimbangkan untuk mengecualikan jenis **`AWS::Config::ResourceCompliance`** sumber daya dari rekaman sebelum menghapus aturan

Menghapus aturan membuat item konfigurasi (CIs) untuk `AWS::Config::ResourceCompliance` itu dapat memengaruhi biaya Anda untuk perekam konfigurasi. Jika Anda menghapus aturan yang mengevaluasi sejumlah besar jenis sumber daya, ini dapat menyebabkan lonjakan jumlah CIs yang direkam.

Untuk menghindari biaya terkait, Anda dapat memilih untuk menonaktifkan perekaman untuk jenis `AWS::Config::ResourceCompliance` sumber daya sebelum menghapus aturan, dan mengaktifkan kembali perekaman setelah aturan dihapus.

Namun, karena menghapus aturan adalah proses asinkron, mungkin perlu satu jam atau lebih untuk menyelesaikannya. Selama perekaman dinonaktifkan`AWS::Config::ResourceCompliance`, evaluasi aturan tidak akan dicatat dalam riwayat sumber daya terkait.

AWS Config merekomendasikan agar Anda mempertimbangkan faktor-faktor ini case-by-case berdasarkan sebelum memutuskan bagaimana melanjutkan dengan menghapus aturan.

Rekomendasi: Tambahkan logika untuk menangani evaluasi sumber daya yang dihapus untuk aturan lambda khusus

Saat membuat aturan lambda AWS Config kustom, sangat disarankan agar Anda menambahkan logika untuk menangani evaluasi sumber daya yang dihapus.

Ketika hasil evaluasi ditandai sebagai`NOT_APPLICABLE`, mereka akan ditandai untuk dihapus dan dibersihkan. Jika TIDAK ditandai sebagai`NOT_APPLICABLE`, hasil evaluasi akan tetap tidak berubah sampai aturan dihapus, yang dapat menyebabkan lonjakan tak terduga dalam pembuatan CIs for on rule `AWS::Config::ResourceCompliance` deletion.

Untuk informasi tentang cara menyetel aturan lambda AWS Config kustom agar ditampilkan untuk sumber daya yang `NOT_APPLICABLE` dihapus, lihat Mengelola sumber daya yang dihapus dengan aturan lambda AWS Config kustom.

Rekomendasi: Menyediakan sumber daya dalam cakupan untuk aturan lambda khusus

AWS Config Aturan Lambda Kustom dapat menyebabkan sejumlah besar pemanggilan fungsi Lambda jika aturan tidak dicakup ke satu atau beberapa jenis sumber daya. Untuk menghindari peningkatan aktivitas yang terkait dengan akun Anda, sangat disarankan untuk menyediakan sumber daya dalam cakupan aturan Lambda Kustom Anda. Jika tidak ada jenis sumber daya yang dipilih, aturan akan memanggil fungsi Lambda untuk semua sumber daya di akun.

Other considerations

Defaut Nilai untuk Aturan Terkelola

Nilai default yang ditentukan untuk aturan terkelola hanya diisi sebelumnya saat menggunakan konsol. AWS Nilai default tidak disediakan untuk API, CLI, atau SDK.

Penundaan Perekaman Item Konfigurasi

AWS Config biasanya mencatat perubahan konfigurasi ke sumber daya Anda tepat setelah perubahan terdeteksi, atau pada frekuensi yang Anda tentukan. Namun, ini atas dasar upaya terbaik dan kadang-kadang bisa memakan waktu lebih lama. Misalnya, jenis sumber daya dengan penundaan yang diketahui adalah`AWS::SecretsManager::Secret`. Jenis sumber daya ini adalah contoh, dan daftar ini tidak lengkap.

Kebijakan dan hasil kepatuhan

Kebijakan IAM dan kebijakan lain yang dikelola AWS Organizations dapat memengaruhi apakah AWS Config memiliki izin untuk merekam perubahan konfigurasi untuk sumber daya Anda. Selain itu, aturan secara langsung mengevaluasi konfigurasi sumber daya dan aturan tidak memperhitungkan kebijakan ini saat menjalankan evaluasi. Pastikan bahwa kebijakan yang berlaku selaras dengan cara Anda ingin menggunakan AWS Config.

Menandai dukungan untuk jenis sumber daya

Jika tipe sumber daya tidak mendukung penandaan atau tidak menyertakan informasi tag dalam respons API deskripsinya, tidak AWS Config akan menangkap data tag dalam item konfigurasi (CIs) untuk jenis sumber daya tersebut. AWS Config masih akan mencatat sumber daya ini. Namun, fungsionalitas apa pun yang bergantung pada data tag tidak akan berfungsi. Ini memengaruhi pemfilteran, pengelompokan, atau evaluasi kepatuhan berbasis tag yang bergantung pada data tag.

Bucket Direktori Tidak Didukung

Aturan terkelola hanya mendukung bucket tujuan umum saat mengevaluasi sumber daya Amazon Simple Storage Service (Amazon S3). Untuk informasi selengkapnya tentang bucket tujuan umum dan bucket direktori, lihat Ikhtisar bucket dan Bucket direktori di Panduan Pengguna Amazon S3.

Aturan Terkelola dan Jenis Sumber Daya IAM Global

Jenis sumber daya IAM global yang tersedia sebelum Februari 2022 (`AWS::IAM::Group`,, `AWS::IAM::Policy``AWS::IAM::Role`, dan`AWS::IAM::User`) hanya dapat direkam oleh AWS

Config di AWS Wilayah yang tersedia sebelum AWS Config Februari 2022. Jenis sumber daya ini tidak dapat dicatat di Wilayah yang didukung AWS Config setelah Februari 2022. Untuk daftar Wilayah tersebut, lihat Merekam AWS Sumber Daya | Sumber Daya Global.

Jika Anda merekam jenis sumber daya IAM global di setidaknya satu Wilayah, aturan periodik yang melaporkan kepatuhan pada jenis sumber daya IAM global akan menjalankan evaluasi di semua Wilayah di mana aturan periodik ditambahkan, bahkan jika Anda belum mengaktifkan pencatatan jenis sumber daya IAM global di Wilayah tempat aturan periodik ditambahkan.

Untuk menghindari evaluasi yang tidak perlu, Anda hanya harus menerapkan aturan berkala yang melaporkan kepatuhan pada jenis sumber daya IAM global ke salah satu Wilayah yang didukung. Untuk daftar aturan terkelola yang didukung di Wilayah mana, lihat Daftar Aturan AWS Config Terkelola menurut Ketersediaan Wilayah.

Support Wilayah

Saat ini, fitur AWS Config Aturan didukung di AWS wilayah berikut. Untuk daftar AWS Config aturan individual yang didukung di Wilayah mana, lihat Daftar Aturan AWS Config Terkelola menurut Ketersediaan Wilayah.

Nama Wilayah	Wilayah	Titik Akhir	Protokol
AS Timur (Ohio)	us–east-2	config.us-east-2.amazonaws.com	HTTPS
		config-fips.us-east-2.amazonaws.com	HTTPS
AS Timur (Virginia Utara)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
		config-fips.us-east-1.amazonaws.com	HTTPS
AS Barat (Californ ia Utara)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
		config-fips.us-west-1.amazonaws.com	HTTPS
AS Barat (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
		config-fips.us-west-2.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Afrika (Cape Town)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asia Pasifik (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asia Pasifik (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asia Pasifik (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asia Pasifik (Malaysia)	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS
Asia Pasifik (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia Pasifik (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pasifik (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Asia Pasifik (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia Pasifik (Singapura)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pasifik (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pasifik (Taipei)	ap-timur-2	config.ap-east-2.amazonaws.com	HTTPS
Asia Pasifik (Thailand)	ap-tenggara 7	config.ap-southeast-7.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Kanada (Pusat)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Kanada Barat (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Eropa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Eropa (Irlandia)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Eropa (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Eropa (Milan)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Eropa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Eropa (Spanyol)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Eropa (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Eropa (Zürich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Meksiko (Tengah)	mx-pusat-1	config.mx-central-1.amazonaws.com	HTTPS
Timur Tengah (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Timur Tengah (UAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Amerika Selatan (Sao Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (AS-Timur)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (AS-Barat)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Menerapkan AWS Config Aturan di seluruh akun anggota di AWS Organisasi didukung di Wilayah berikut.

Nama Wilayah	Wilayah	Titik Akhir	Protokol
AS Timur (Ohio)	us–east-2	config.us-east-2.amazonaws.com	HTTPS
AS Timur (Virginia Utara)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
AS Barat (Californ ia Utara)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
AS Barat (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Afrika (Cape Town)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asia Pasifik (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asia Pasifik (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asia Pasifik (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asia Pasifik (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia Pasifik (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pasifik (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia Pasifik (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Asia Pasifik (Singapura)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pasifik (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Kanada (Pusat)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Kanada Barat (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Eropa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Eropa (Irlandia)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Eropa (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Eropa (Milan)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Eropa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Eropa (Spanyol)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Eropa (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Eropa (Zürich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Timur Tengah (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Timur Tengah (UAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
Amerika Selatan (Sao Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (AS-Timur)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (AS-Barat)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Komponen AWS Config Aturan

AWS Config aturan mengevaluasi pengaturan konfigurasi AWS sumber daya Anda. Halaman ini membahas komponen aturan.

Topik

- Bagaimana AWS Config Aturan Bekerja
- Jenis Pemicu
- Mode Evaluasi
- AWS Config Metadata Aturan

Bagaimana AWS Config Aturan Bekerja

Meskipun AWS Config terus melacak perubahan konfigurasi yang terjadi di antara sumber daya Anda, ia memeriksa apakah perubahan ini tidak sesuai dengan ketentuan dalam aturan Anda. Jika sumber daya tidak mematuhi aturan, AWS Config tandai sumber daya dan aturan sebagai tidak sesuai.

Ada empat kemungkinan hasil evaluasi untuk suatu AWS Config aturan.

Hasil evaluasi	Deskripsi
`COMPLIANT`	Aturan melewati kondisi pemeriksaan kepatuhan.
`NON_COMPLIANT`	Aturan gagal dalam kondisi pemeriksaan kepatuhan.
`ERROR`	Salah satu parameter yang diperlukan/opsional tidak valid, bukan dari jenis yang benar, atau diformat secara tidak benar.
`NOT_APPLICABLE`	Digunakan untuk menyaring sumber daya yang logika aturan tidak dapat diterapkan. Misalnya, alb-desync-mode-checkaturan hanya memeriksa Application Load Balancers, dan

Hasil evaluasi	Deskripsi
	mengabaikan Network Load Balancers dan Gateway Load Balancers.

Misalnya, ketika EC2 volume dibuat, AWS Config dapat mengevaluasi volume terhadap aturan yang membutuhkan volume untuk dienkripsi. Jika volume tidak dienkripsi, AWS Config tandai volume dan aturan sebagai tidak sesuai. AWS Config juga dapat memeriksa semua sumber daya Anda untuk persyaratan seluruh akun. Misalnya, AWS Config dapat memeriksa apakah jumlah EC2 volume dalam akun tetap dalam total yang diinginkan, atau apakah akun digunakan AWS CloudTrail untuk logging.

Jenis Pemicu

Setelah Anda menambahkan aturan ke akun Anda, AWS Config bandingkan sumber daya Anda dengan ketentuan aturan. Setelah evaluasi awal ini, AWS Config terus jalankan evaluasi setiap kali dipicu. Pemicu evaluasi didefinisikan sebagai bagian dari aturan, dan mereka dapat mencakup jenis berikut.

Jenis pemicu	Deskripsi
Perubahan konfigurasi	AWS Config menjalankan evaluasi untuk aturan ketika ada sumber daya yang cocok dengan cakupan aturan dan ada perubahan konfigura si sumber daya. Evaluasi berjalan setelah AWS Config mengirimkan pemberitahuan perubahan item konfigurasi. Anda memilih sumber daya mana yang memulai evaluasi dengan menentukan ruang lingkup aturan. Ruang lingkup dapat mencakup yang berikut: • Satu atau lebih jenis sumber daya • Kombinasi tipe sumber daya dan ID sumber daya • Kombinasi kunci tag dan nilai

Jenis pemicu	Deskripsi
	• Ketika sumber daya yang direkam dibuat, diperbarui, atau dihapus AWS Config menjalankan evaluasi saat mendeteksi perubahan pada sumber daya yang cocok dengan cakupan aturan. Anda dapat menggunakan ruang lingkup untuk menentukan sumber daya mana yang memulai evaluasi.
Berkala	AWS Config menjalankan evaluasi untuk aturan pada frekuensi yang Anda pilih; misalnya, setiap 24 jam.
Hibrida	Beberapa aturan memiliki perubahan konfigura si dan pemicu periodik. Untuk aturan ini, AWS Config evaluasi sumber daya Anda saat mendeteksi perubahan konfigurasi dan juga pada frekuensi yang Anda tentukan.

Mode Evaluasi

Ada dua mode evaluasi untuk AWS Config aturan.

Mode evaluasi	Deskripsi
Proaktif	Gunakan evaluasi proaktif untuk mengevalu asi sumber daya sebelum digunakan. Ini memungkinkan Anda untuk mengevaluasi apakah satu set properti sumber daya, jika digunakan untuk mendefinisikan AWS sumber daya, akan COMPLIANT atau NON_COMPL IANT mengingat seperangkat aturan proaktif yang Anda miliki di akun Anda di Wilayah Anda.

Mode evaluasi	Deskripsi
Detective	Gunakan evaluasi detektif untuk mengevaluasi sumber daya yang telah digunakan. Ini memungkinkan Anda untuk mengevaluasi pengaturan konfigurasi sumber daya yang ada.

> **Note**
>
> Aturan proaktif tidak memulihkan sumber daya yang ditandai sebagai NON_COMPLIANT atau mencegahnya diterapkan.

Untuk informasi selengkapnya, lihat Mengaktifkan Evaluasi Proaktif untuk AWS Config Aturan.

Daftar aturan terkelola dengan evaluasi proaktif

Untuk daftar aturan terkelola yang mendukung evaluasi proaktif, lihat Daftar Aturan AWS Config Terkelola menurut Mode Evaluasi.

Daftar jenis sumber daya yang didukung untuk evaluasi proaktif

Berikut ini adalah daftar jenis sumber daya yang didukung untuk evaluasi proaktif:

- `AWS::ApiGateway::Stage`
- `AWS::AutoScaling::AutoScalingGroup`
- `AWS::EC2::EIP`
- `AWS::EC2::Instance`
- `AWS::EC2::Subnet`
- `AWS::Elasticsearch::Domain`
- `AWS::Lambda::Function`
- `AWS::RDS::DBInstance`
- `AWS::Redshift::Cluster`
- `AWS::S3::Bucket`
- `AWS::SNS::Topic`

AWS Config Metadata Aturan

AWS Config aturan dapat berisi metadata yang dapat berubah berikut:

DefaultName

DefaultName adalah nama yang instance aturan akan mendapatkan secara default.

deskripsi

Deskripsi aturan memberikan konteks untuk apa yang dievaluasi aturan. AWS Config Konsol memiliki batas 256 karakter. Sebagai praktik terbaik, deskripsi aturan harus dimulai dengan “Memeriksa jika” dan menyertakan deskripsi skenario NON_COMPLIANT. Nama Layanan harus ditulis di awal penuh dengan AWS atau Amazon ketika pertama kali disebutkan dalam deskripsi aturan. Misalnya, AWS CloudTrail atau Amazon CloudWatch sebagai pengganti CloudTrail atau CloudWatch untuk penggunaan pertama. Nama layanan dapat disingkat setelah referensi berikutnya.

ruang lingkup

Ruang lingkup menentukan jenis sumber daya yang ditargetkan aturan. Untuk daftar jenis sumber daya yang didukung, lihat Jenis Sumber Daya yang Didukung.

compulsoryInputParameterDetail

compulsoryInputParameterDetail digunakan untuk parameter yang diperlukan untuk aturan untuk melakukan evaluasinya. Misalnya, aturan `access-keys-rotated` terkelola termasuk `maxAccessKeyAge` sebagai parameter yang diperlukan. Jika parameter diperlukan, itu tidak akan ditandai sebagai (Opsional). Untuk setiap parameter, tipe harus ditentukan. Jenis dapat berupa salah satu dari “String”, “int”, “double”, “CSV”, “boolean” dan "StringMap”.

optionalInputParameterDetail

optionalInputParameterDetail digunakan untuk parameter yang opsional untuk aturan untuk melakukan evaluasinya. Misalnya, aturan `elasticsearch-logs-to-cloudwatch` terkelola termasuk `logTypes` sebagai parameter opsional. Untuk setiap parameter, tipe harus ditentukan. Jenis dapat berupa salah satu dari “String”, “int”, “double”, “CSV”, “boolean” dan "StringMap”.

supportedEvaluationModes

supportedEvaluationModes Penentuan kapan sumber daya akan dievaluasi, baik sebelum sumber daya telah digunakan atau setelah sumber daya telah digunakan.

`DETECTIVE`digunakan untuk mengevaluasi sumber daya yang telah digunakan. Ini memungkinkan Anda untuk mengevaluasi pengaturan konfigurasi sumber daya yang ada. `PROACTIVE`digunakan untuk mengevaluasi sumber daya sebelum digunakan.

Ini memungkinkan Anda untuk mengevaluasi apakah satu set properti sumber daya, jika digunakan untuk mendefinisikan AWS sumber daya, akan COMPLIANT atau NON_COMPLIANT mengingat seperangkat aturan proaktif yang Anda miliki di akun Anda di Wilayah Anda.

Anda dapat menentukan supportedEvaluationModes ke`DETECTIVE`,`PROACTIVE`, atau keduanya `DETECTIVE` dan`PROACTIVE`. Anda harus menentukan mode evaluasi dan bidang ini tidak dapat tetap kosong.

> **Note**
>
> Aturan proaktif tidak memulihkan sumber daya yang ditandai sebagai NON_COMPLIANT atau mencegahnya diterapkan.

AWS Config Aturan yang Dikelola

AWS Config menyediakan aturan AWS terkelola, yang merupakan aturan yang telah ditentukan sebelumnya dan dapat disesuaikan yang AWS Config digunakan untuk mengevaluasi apakah AWS sumber daya Anda mematuhi praktik terbaik umum. Misalnya, Anda dapat menggunakan aturan terkelola untuk mulai menilai dengan cepat apakah volume Amazon Elastic Block Store (Amazon EBS) Anda dienkripsi atau apakah tag tertentu diterapkan ke sumber daya Anda.

AWS Config Konsol memandu Anda melalui proses mengonfigurasi dan mengaktifkan aturan terkelola. Anda juga dapat menggunakan AWS Config API AWS Command Line Interface atau untuk meneruskan kode JSON yang mendefinisikan konfigurasi aturan terkelola Anda.

Anda dapat menyesuaikan perilaku aturan terkelola agar sesuai dengan kebutuhan Anda. Misalnya, Anda dapat menentukan cakupan aturan untuk membatasi sumber daya mana yang memicu evaluasi aturan, seperti EC2 instance atau volume.

Anda dapat menyesuaikan parameter aturan untuk menentukan atribut yang harus dimiliki sumber daya Anda untuk mematuhi aturan. Misalnya, Anda dapat menyesuaikan parameter untuk menentukan bahwa grup keamanan Anda harus memblokir lalu lintas masuk ke nomor port tertentu.

Sebelum menggunakan aturan terkelola, lihatPertimbangan.

Topik

- Daftar Aturan AWS Config Terkelola
- Daftar Aturan AWS Config Terkelola berdasarkan Mode Evaluasi
- Daftar Aturan AWS Config Terkelola berdasarkan Jenis Pemicu
- Daftar Aturan AWS Config Terkelola berdasarkan Ketersediaan Wilayah
- Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template

Daftar Aturan AWS Config Terkelola

AWS Config saat ini mendukung aturan terkelola berikut. Sebelum menggunakan aturan ini, lihatPertimbangan.

Topik

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-diaktifkan
- alb-http-to-https-pemeriksaan-pengalihan
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-penghapusan-diaktifkan
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-diaktifkan
- amplify-branch-tagged

- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-tidak-kosong
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-penyimpanan
- appconfig-hosted-configuration-version-deskripsi
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-penerusan
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-default-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged

- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-akses
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-saat istirahat
- appsync-cache-ct-encryption-dalam transit
- appsync-cache-encryption-at-istirahat
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-istirahat
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging

- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapusan-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-diaktifkan
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-periksa
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf

- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-dikonfigurasi
- cloudfront-no-deprecated-ssl-protokol
- cloudfront-origin-access-identity-diaktifkan
- cloudfront-origin-failover-enabled
- cloudfront-s3- origin-access-control-enabled
- cloudfront-s3- origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-dienkripsi
- cloudfront-viewer-policy-https
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloudtrail-diaktifkan
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-periksa

- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- codedeploy-auto-rollback-monitor-diaktifkan
- codedeploy-deployment-group-auto-rollback-diaktifkan
- codedeploy-deployment-group-outdated-instances-pembaruan
- codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-akses-cek
- cognito-user-pool-advanced-keamanan diaktifkan
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-pembuatan profil
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-Terlampir
- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy

- desired-instance-type
- dms-auto-minor-version-tingkatkan periksa
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-diaktifkan
- dms-neptune-iam-authorization-diaktifkan
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-diaktifkan
- docdb-cluster-backup-retention-periksa
- docdb-cluster-deletion-protection-diaktifkan
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-dilarang
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target

- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- diaktifkan client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -semua client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- diaktifkan enis-source-destination-check
- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- -manajer instance-managed-by-systems
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -dibuat last-backup-recovery-point
- ec2- 2-periksa launch-template-imdsv
- ec2- launch-template-public-ip -dinonaktifkan
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -periksa managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check

- ec2- meets-restore-time-target
- ec2- network-insights-access-scope -analisis ditandai
- ec2- -ditandai network-insights-access-scope
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2- resources-in-logically-air -gapped-lemari besi
- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2- security-group-attached-to -eni-periodik
- ec2- - spot-fleet-request-ct encryption-at-rest
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan
- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled

- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi
- ecs-task-definition-memory-batas-keras
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-pengguna
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan
- terlampir eip
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versi
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted

- elasticache_automatic_backup_check_enabled
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan
- elasticache-repl-grp-encrypted-saat istirahat
- elasticache-repl-grp-encrypted-dalam transit
- elasticache-repl-grp-redis-auth-diaktifkan
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-logs-to-jam tangan awan
- elastic-beanstalk-managed-updates-diaktifkan
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -periksa predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya

- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-istirahat
- emr-security-configuration-encryption-transit
- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-konfigurasi-ada
- fis-experiment-template-tagged
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-dibuat
- fsx-lustre-copy-tagsuntuk cadangan
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-audit-log-dikonfigurasi

- fsx-windows-deployment-type-periksa
- glb-listener-tagged
- global-endpoint-event-replication-diaktifkan
- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-tindakan
- iam-external-access-analyzer-diaktifkan
- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa
- iam-oidc-provider-tagged
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa
- iam-root-access-key-periksa

- iam-saml-provider-tagged
- iam-server-certificate-expiration-periksa
- iam-server-certificate-tagged
- iam-user-group-membership-periksa
- iam-user-mfa-enabled
- iam-user-no-policies-periksa
- iam-user-unused-credentials-periksa
- terbatas-ssh
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-diaktifkan
- inspector-lambda-standard-scan-diaktifkan
- ec2- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged

- iot-authorizer-token-signing-diaktifkan
- ivs-channel-playback-authorization-diaktifkan
- ivs-channel-tagged
- ivs-playback-key-pair-ditandai
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-penemuan-cek
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-log
- mfa-enabled-for-iam-akses konsol
- mq-active-broker-ldap-otentikasi
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade diaktifkan
- mq-auto-minor-version-upgrade diaktifkan

- mq-broker-general-logging-diaktifkan
- mq-cloudwatch-audit-logging-diaktifkan
- mq-cloudwatch-audit-log-diaktifkan
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-dinonaktifkan
- msk-connect-connector-logging-diaktifkan
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- msk-unrestricted-access-check
- multi-region-cloudtrail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-periksa
- neptune-cluster-cloudwatch-log-ekspor diaktifkan
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-diaktifkan
- neptune-cluster-encrypted
- neptune-cluster-iam-database-otentikasi
- neptune-cluster-multi-az-diaktifkan
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-dilarang
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan

- nlb-cross-zone-load-menyeimbangkan diaktifkan
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-toleransi
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-pemeriksaan enkripsi-
- opensearch-primary-node-fault-toleransi
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-aurora-postgresql-logske cloudwatch
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-db-security-group-tidak diizinkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan

- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-diaktifkan
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check

- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-serverless-default-admin-periksa
- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi
- redshift-serverless-publish-logske cloudwatch
- redshift-serverless-workgroup-encrypted-dalam transit
- redshift-serverless-workgroup-no-akses publik
- redshift-serverless-workgroup-routes-dalam-vpc
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-common-ports
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- rute53- query-logging-enabled
- s3 -aturan-periksa express-dir-bucket-lifecycle
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check

- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-ember dengan tag
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -gapped-lemari besi
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-ditandai
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi

- sagemaker-notebook-instance-root-akses-cek
- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-notifikasi-diaktifkan
- sns-topic-no-public-akses
- sqs-queue-no-public-akses
- ssm-automation-block-public-berbagi
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description

- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-dibuat
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-rencana cadangan
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-peering-dns-resolution-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- vpc-vpn-2-terowongan
- wafv2-logging diaktifkan
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-kosong
- waf-global-rule-not-kosong
- waf-global-webacl-not-kosong
- waf-regional-rulegroup-not-kosong
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong
- workspaces-root-volume-encryption-diaktifkan

- workspaces-user-volume-encryption-diaktifkan

access-keys-rotated

Memeriksa apakah kunci akses IAM aktif diputar (diubah) dalam jumlah hari yang ditentukan dalam. `maxAccessKeyAge` Aturannya adalah NON_COMPLIANT jika kunci akses tidak diputar dalam jangka waktu yang ditentukan. Nilai default adalah 90 hari.

> **Warning**
>
> Jangan berikan kunci akses Anda kepada pihak yang tidak berwenang, bahkan untuk membantu menemukan pengenal akun Anda. Dengan melakukan tindakan ini, Anda mungkin memberi seseorang akses permanen ke akun Anda. Praktik terbaik keamanan adalah untuk menghapus kata sandi dan access key saat pengguna tidak lagi membutuhkannya.

> **Note**
>
> Jenis Sumber Daya Ditandai sebagai Tidak Sesuai di Konsol
> Jika aturan ini menemukan bahwa salah satu kunci akses Anda tidak sesuai, jenis `AWS::IAM::User` sumber daya juga akan ditandai sebagai tidak sesuai di konsol. AWS Aturan Terkelola dan Jenis Sumber Daya IAM Global
> Jenis sumber daya IAM global yang tersedia sebelum Februari 2022 (`AWS::IAM::Group`,, `AWS::IAM::PolicyAWS::IAM::Role`, dan`AWS::IAM::User`) hanya dapat direkam oleh AWS Config di AWS Wilayah yang tersedia sebelum AWS Config Februari 2022. Jenis sumber daya ini tidak dapat dicatat di Wilayah yang didukung AWS Config setelah Februari 2022. Untuk daftar Wilayah tersebut, lihat Merekam AWS Sumber Daya | Sumber Daya Global.
> Jika Anda merekam jenis sumber daya IAM global di setidaknya satu Wilayah, aturan periodik yang melaporkan kepatuhan pada jenis sumber daya IAM global akan menjalankan evaluasi di semua Wilayah di mana aturan periodik ditambahkan, bahkan jika Anda belum mengaktifkan pencatatan jenis sumber daya IAM global di Wilayah tempat aturan periodik ditambahkan.
> Untuk menghindari evaluasi yang tidak perlu, Anda hanya harus menerapkan aturan berkala yang melaporkan kepatuhan pada jenis sumber daya IAM global ke salah satu Wilayah yang didukung. Untuk daftar aturan terkelola yang didukung di Wilayah mana, lihat Daftar Aturan AWS Config Terkelola menurut Ketersediaan Wilayah.

Batasan
Aturan ini tidak berlaku untuk kunci akses pengguna root AWS akun. Untuk menghapus atau memutar kunci akses pengguna root Anda, gunakan kredensi pengguna root Anda untuk masuk ke halaman My Security Credentials di at. AWS Management Console https://aws.amazon.com/console/

Pengidentifikasi: ACCESS_KEYS_ROTATED

Jenis Sumber Daya: AWS::IAM::User

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

maxAccessKeyUmur, Jenis: int, Default: 90

Jumlah hari maksimum tanpa rotasi. Default 90.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

account-part-of-organizations

Memeriksa apakah AWS akun merupakan bagian dari AWS Organizations. Aturannya adalah NON_COMPLIANT jika AWS akun bukan bagian dari ID akun master Organizations AWS atau AWS Organizations tidak cocok dengan parameter aturan. `MasterAccountId`

Note

Aturan Terkelola dan Jenis Sumber Daya IAM Global
Jenis sumber daya IAM global yang tersedia sebelum Februari 2022 (`AWS::IAM::Group`,, `AWS::IAM::PolicyAWS::IAM::Role`, dan`AWS::IAM::User`) hanya dapat direkam

oleh AWS Config di AWS Wilayah yang tersedia sebelum AWS Config Februari 2022. Jenis sumber daya ini tidak dapat dicatat di Wilayah yang didukung AWS Config setelah Februari 2022. Untuk daftar Wilayah tersebut, lihat Merekam AWS Sumber Daya | Sumber Daya Global.

Jika Anda merekam jenis sumber daya IAM global di setidaknya satu Wilayah, aturan periodik yang melaporkan kepatuhan pada jenis sumber daya IAM global akan menjalankan evaluasi di semua Wilayah di mana aturan periodik ditambahkan, bahkan jika Anda belum mengaktifkan pencatatan jenis sumber daya IAM global di Wilayah tempat aturan periodik ditambahkan.

Untuk menghindari evaluasi yang tidak perlu, Anda hanya harus menerapkan aturan berkala yang melaporkan kepatuhan pada jenis sumber daya IAM global ke salah satu Wilayah yang didukung. Untuk daftar aturan terkelola yang didukung di Wilayah mana, lihat Daftar Aturan AWS Config Terkelola menurut Ketersediaan Wilayah.

Pengidentifikasi: ACCOUNT_PART_OF_ORGANIZATIONS

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Wilayah Asia Pasifik (Taipei)

Parameter:

MasterAccountId (Opsional), Tipe: String

ID akun master untuk AWS akun.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

acmpca-certificate-authority-tagged

Memeriksa apakah otoritas sertifikat CA AWS Pribadi memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: ACMPCA_CERTIFICATE_AUTHORITY_TAGGED

Jenis Sumber Daya: AWS::ACMPCA::CertificateAuthority

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

acm-certificate-expiration-check

Memeriksa apakah AWS Certificate Manager Certificate di akun Anda ditandai kedaluwarsa dalam jumlah hari yang ditentukan. Sertifikat yang diberikan oleh ACM diperpanjang secara otomatis. ACM tidak secara otomatis memperbarui sertifikat yang Anda impor. Aturannya adalah NON_COMPLIANT jika sertifikat Anda akan kedaluwarsa.

Pengidentifikasi: ACM_CERTIFICATE_EXPIRATION_CHECK

Jenis Sumber Daya: AWS::ACM::Certificate

Jenis pemicu: Perubahan konfigurasi dan Periodik

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Osaka)

Parameter:

daysToExpiration (Opsional), Jenis: int, Default: 14

> Tentukan jumlah hari sebelum aturan menandai Sertifikat ACM sebagai tidak sesuai.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

acm-certificate-rsa-check

Memeriksa apakah sertifikat RSA yang dikelola oleh AWS Certificate Manager (ACM) memiliki panjang kunci minimal '2048' bit. Aturannya adalah NON_COMPLIANT jika panjang kunci minimum kurang dari 2048 bit.

Pengidentifikasi: ACM_CERTIFICATE_RSA_CHECK

Jenis Sumber Daya: AWS::ACM::Certificate

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Tiongkok (Ningxia) Wilayah

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

acm-pca-root-ca-dinonaktifkan

Memeriksa apakah AWS Private Certificate Authority (AWS Private CA) memiliki CA root yang dinonaktifkan. Aturannya adalah NON_COMPLIANT untuk root CAs dengan status yang tidak DINONAKTIFKAN.

Pengidentifikasi: ACM_PCA_ROOT_CA_DISABLED

Jenis Sumber Daya: AWS::ACMPCA::CertificateAuthority

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Tiongkok (Ningxia) Wilayah

Parameter:

dikecualikan CAArns (Opsional), Jenis: CSV

> Daftar Nama Sumber Daya Amazon (ARN) CA yang dipisahkan koma yang dapat diaktifkan. Nilai ini dapat diberikan untuk yang lain CAs, seperti root tertentu CAs atau CA perantara yang dapat diaktifkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

active-mq-supported-version

Memeriksa apakah broker Amazon MQ ActiveMQ berjalan pada versi mesin minimum yang didukung. Aturannya adalah NON_COMPLIANT jika broker ActiveMQ tidak berjalan pada versi mesin minimum yang didukung yang Anda tentukan.

Pengidentifikasi: ACTIVE_MQ_SUPPORTED_VERSION

Jenis Sumber Daya: AWS::AmazonMQ::Broker

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

supportedEngineVersion, Tipe: String

> Nilai string untuk aturan untuk memeriksa versi mesin minimum yang didukung untuk broker ActiveMQ. Broker ActiveMQ menggunakan spesifikasi versi semantik: XYZ X menunjukkan versi utama, Y mewakili versi minor, dan Z menunjukkan versi patch.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

alb-desync-mode-check

Memeriksa apakah Application Load Balancer (ALB) dikonfigurasi dengan mode mitigasi desync yang ditentukan pengguna. Aturannya adalah NON_COMPLIANT jika mode mitigasi desync ALB tidak cocok dengan mode mitigasi desync yang ditentukan pengguna.

Pengidentifikasi: ALB_DESYNC_MODE_CHECK

Jenis Sumber Daya: AWS::ElasticLoadBalancingV2::LoadBalancer

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

DesyncMode, Jenis: CSV

> Daftar yang dipisahkan koma, di mana pelanggan dapat memilih maksimal 2 nilai antara - 'defensif', 'ketat', dan 'monitor'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

alb-http-drop-invalid-header-diaktifkan

Memeriksa apakah aturan mengevaluasi AWS Application Load Balancers (ALB) untuk memastikan mereka dikonfigurasi untuk menjatuhkan header http. Aturannya adalah NON_COMPLIANT jika nilai routing.http.drop_invalid_header_fields.enabled disetel ke false.

Pengidentifikasi: ALB_HTTP_DROP_INVALID_HEADER_ENABLED

Jenis Sumber Daya: AWS::ElasticLoadBalancingV2::LoadBalancer

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Osaka)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

alb-http-to-https-pemeriksaan-pengalihan

Memeriksa apakah pengalihan HTTP ke HTTPS dikonfigurasi pada semua pendengar HTTP Application Load Balancers. Aturannya adalah NON_COMPLIANT jika satu atau beberapa pendengar HTTP Application Load Balancer tidak memiliki pengalihan HTTP ke HTTPS yang dikonfigurasi. Aturannya juga NON_COMPLIANT jika salah satu pendengar HTTP lainnya memiliki penerusan ke pendengar HTTP alih-alih pengalihan.

Pengidentifikasi: ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK

Jenis Sumber Daya: AWS::ElasticLoadBalancingV2::LoadBalancer

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Osaka)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

alb-internal-scheme-check

Memeriksa apakah skema Application Load Balancer bersifat internal. Aturannya adalah NON_COMPLIANT jika configuration.scheme tidak disetel ke internal.

Pengidentifikasi: ALB_INTERNAL_SCHEME_CHECK

Jenis Sumber Daya: AWS::ElasticLoadBalancingV2::LoadBalancer

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

alb-listener-tagged

Memeriksa apakah pendengar Application Load Balancer memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: ALB_LISTENER_TAGGED

Jenis Sumber Daya: AWS::ElasticLoadBalancingV2::Listener

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

alb-waf-enabled

Memeriksa apakah AWS WAF diaktifkan pada Application Load Balancers (). ALBs Aturannya adalah NON_COMPLIANT jika key: waf.enabled disetel ke false.

Pengidentifikasi: ALB_WAF_ENABLED

Jenis Sumber Daya: AWS::ElasticLoadBalancingV2::LoadBalancer

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Osaka)

Parameter:

wafWebAclIds (Opsional), Jenis: CSV

> Daftar terpisah koma dari ID ACL web (untuk WAF) atau web ACL ARN (untuk WAFV2) memeriksa asosiasi ALB.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

amplify-app-branch-auto-penghapusan-diaktifkan

Memeriksa apakah aplikasi AWS Amplify secara otomatis memutuskan cabang di Amplify Hosting saat Anda menghapus cabang dari repositori Git Anda. Aturannya adalah NON_COMPLIANT jika konfigurasi. EnableBranchAutoDeletion adalah palsu.

Pengidentifikasi: AMPLIFY_APP_BRANCH_AUTO_DELETION_ENABLED

Jenis Sumber Daya: AWS::Amplify::App

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Afrika (Cape Town), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

amplify-app-description

Memeriksa apakah aplikasi AWS Amplify memiliki deskripsi. Aturannya adalah NON_COMPLIANT jika Configuration.description tidak ada atau string kosong.

Pengidentifikasi: AMPLIFY_APP_DESCRIPTION

Jenis Sumber Daya: AWS::Amplify::App

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Afrika (Cape Town), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

amplify-app-tagged

Memeriksa apakah aplikasi AWS Amplify memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk aturan tersebut. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: AMPLIFY_APP_TAGGED

Jenis Sumber Daya: AWS::Amplify::App

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Afrika (Cape Town), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

amplify-branch-performance-mode-diaktifkan

Memeriksa apakah cabang AWS Amplify mengaktifkan mode kinerja. Aturannya adalah NON_COMPLIANT jika konfigurasi. EnablePerformanceMode adalah palsu.

Pengidentifikasi: AMPLIFY_BRANCH_PERFORMANCE_MODE_ENABLED

Jenis Sumber Daya: AWS::Amplify::Branch

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Afrika (Cape Town), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

amplify-branch-tagged

Memeriksa apakah cabang AWS Amplify memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk aturan tersebut. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: AMPLIFY_BRANCH_TAGGED

Jenis Sumber Daya: AWS::Amplify::Branch

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Afrika (Cape Town), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

api-gwv2- access-logs-enabled

Memeriksa apakah tahapan Amazon API Gateway V2 mengaktifkan pencatatan akses. Aturannya adalah NON_COMPLIANT jika 'accessLogSettings' tidak ada dalam konfigurasi Stage.

Pengidentifikasi: 2_ACCESS_LOGS_ENABLED API_GWV

Jenis Sumber Daya: AWS::ApiGatewayV2::Stage

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur), AWS GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

api-gwv2- authorization-type-configured

Memeriksa apakah rute API Amazon API Gatewayv2 memiliki jenis otorisasi yang ditetapkan. Aturan ini NON_COMPLIANT jika jenis otorisasi adalah NONE.

Pengidentifikasi: 2_AUTHORIZATION_TYPE_CONFIGURATED API_GWV

Jenis Sumber Daya: AWS::ApiGatewayV2::Route

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik

(Melbourne), (AS-Timur), AWS GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

AuthorizationType (Opsional), Tipe: String

Parameter untuk memeriksa jenis otorisasi rute API terhadap. Parameter string yang cocok dengan CUSTOM, AWS_IAM, JWT valid.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

api-gw-associated-with-waf

Memeriksa apakah tahap API Amazon API Gateway menggunakan daftar kontrol akses web AWS WAF (web ACL). Aturannya adalah NON_COMPLIANT jika ACL Web AWS WAF tidak digunakan atau jika ACL AWS Web yang digunakan tidak cocok dengan apa yang tercantum dalam parameter aturan.

Pengidentifikasi: _ASSOCIATED_WITH_WAF API_GW

Jenis Sumber Daya: AWS::ApiGateway::Stage

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Meksiko (Tengah), Asia Pasifik (Taipei)

Parameter:

WebAclArns (Opsional), Jenis: CSV

Daftar web ACL Amazon Resource Names ARNs () yang dipisahkan koma.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

api-gw-cache-enabled-dan-dienkripsi

Memeriksa apakah semua metode dalam tahapan Amazon API Gateway telah mengaktifkan cache dan cache dienkripsi. Aturannya adalah NON_COMPLIANT jika metode apa pun dalam tahap Amazon API Gateway tidak dikonfigurasi ke cache atau cache tidak dienkripsi.

Pengidentifikasi: _CACHE_ENABLED_AND_ENCRYPTED API_GW

Jenis Sumber Daya: AWS::ApiGateway::Stage

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Meksiko (Tengah), Asia Pasifik (Taipei)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

api-gw-endpoint-type-periksa

Memeriksa apakah Amazon API Gateway APIs adalah tipe yang ditentukan dalam parameter aturan`endpointConfigurationType`. Aturan mengembalikan NON_COMPLIANT jika REST API tidak cocok dengan tipe titik akhir yang dikonfigurasi dalam parameter aturan.

Pengidentifikasi: API_GW _ENDPOINT_TYPE_CHECK

Jenis Sumber Daya: AWS::ApiGateway::RestApi

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Meksiko (Tengah), Asia Pasifik (Taipei)

Parameter:

endpointConfigurationTypes, Tipe: String

Daftar yang diizinkan dipisahkan koma. endpointConfigurationTypes Nilai yang diizinkan adalah REGIONAL, PRIVATE dan EDGE.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

api-gw-execution-logging-diaktifkan

Memeriksa apakah semua metode dalam tahapan Amazon API Gateway telah mengaktifkan pencatatan. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan, atau jika `loggingLevel` bukan ERROR atau INFO.

Pengidentifikasi: _EXECUTION_LOGGING_ENABLED API_GW

Jenis Sumber Daya: AWS::ApiGateway::Stage, AWS::ApiGatewayV2::Stage

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Meksiko (Tengah), Asia Pasifik (Taipei)

Parameter:

LoggingLevel (Opsional), Tipe: String, Default: ERROR, INFO

Daftar tingkat logging tertentu yang dipisahkan koma (misalnya, ERROR, INFO atau ERROR, INFO).

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

api-gw-ssl-enabled

Memeriksa apakah tahap REST API menggunakan sertifikat SSL. Aturannya adalah NON_COMPLIANT jika tahap REST API tidak memiliki sertifikat SSL terkait.

> **Note**
>
> Aturan ini kembali `NOT_APPLICABLE` jika GetIntegrationAPI kembali `AWS` sebagai tipe.

Pengidentifikasi: _SSL_ENABLED API_GW

Jenis Sumber Daya: AWS::ApiGateway::Stage

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Meksiko (Tengah), Asia Pasifik (Taipei)

Parameter:

Sertifikat IDs (Opsional), Jenis: CSV

Daftar sertifikat klien yang dipisahkan koma yang IDs dikonfigurasi pada tahap REST API.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

api-gw-xray-enabled

Memeriksa apakah penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.

Pengidentifikasi: _XRAY_ENABLED API_GW

Jenis Sumber Daya: AWS::ApiGateway::Stage

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Meksiko (Tengah), Asia Pasifik (Taipei)

Parameter:

Tidak ada

Evaluasi Proaktif

Untuk langkah-langkah tentang cara menjalankan aturan ini dalam mode proaktif, lihat Mengevaluasi Sumber Daya Anda dengan AWS Config Aturan. Agar aturan ini mengembalikan COMPLIANT dalam mode proaktif, skema konfigurasi sumber daya untuk StartResourceEvaluationAPI harus menyertakan input berikut, yang dikodekan sebagai string:

```
"ResourceConfiguration":
...
{
   "TracingEnabled": BOOLEAN,
   "RestApiId": "my-rest-api-Id",
}
...
```

Untuk informasi lebih lanjut tentang evaluasi proaktif, lihat Mode Evaluasi.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

appconfig-application-description

Memeriksa apakah AWS AppConfig aplikasi memiliki deskripsi. Aturannya adalah NON_COMPLIANT jika Configuration.description tidak ada atau string kosong.

Pengidentifikasi: APPCONFIG_APPLICATION_DESCRIPTION

Jenis Sumber Daya: AWS::AppConfig::Application

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Eropa (Zurich) Wilayah

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

appconfig-application-tagged

Memeriksa apakah AWS AppConfig aplikasi memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk diperiksa aturan. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: APPCONFIG_APPLICATION_TAGGED

Jenis Sumber Daya: AWS::AppConfig::Application

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Eropa (Zurich) Wilayah

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

appconfig-configuration-profile-tagged

Memeriksa apakah profil AWS AppConfig konfigurasi memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: APPCONFIG_CONFIGURATION_PROFILE_TAGGED

Jenis Sumber Daya: AWS::AppConfig::ConfigurationProfile

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Eropa (Zurich) Wilayah

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

appconfig-configuration-profile-validators-tidak-kosong

Memeriksa apakah profil AWS AppConfig konfigurasi menyertakan setidaknya satu validator untuk pemeriksaan sintaksis atau semantik untuk memastikan fungsi penerapan konfigurasi sebagaimana dimaksud. Aturannya adalah NON_COMPLIANT jika properti Validators adalah array kosong.

Pengidentifikasi: APPCONFIG_CONFIGURATION_PROFILE_VALIDATORS_NOT_EMPTY

Jenis Sumber Daya: AWS::AppConfig::ConfigurationProfile

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Eropa (Zurich) Wilayah

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

appconfig-deployment-strategy-description

Memeriksa apakah strategi AWS AppConfig penerapan memiliki deskripsi. Aturannya adalah NON_COMPLIANT jika Configuration.description tidak ada atau string kosong.

Pengidentifikasi: APPCONFIG_DEPLOYMENT_STRATEGY_DESCRIPTION

Jenis Sumber Daya: AWS::AppConfig::DeploymentStrategy

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

appconfig-deployment-strategy-replicateuntuk-ssm

Memeriksa apakah strategi AWS AppConfig penyebaran menyimpan strategi penyebaran ke dokumen AWS Systems Manager (SSM). Aturannya adalah NON_COMPLIANT jika konfigurasi. ReplicateTo bukan 'SSM_DOCUMENT'.

Pengidentifikasi: APPCONFIG_DEPLOYMENT_STRATEGY_REPLICATE_TO_SSM

Jenis Sumber Daya: AWS::AppConfig::DeploymentStrategy

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

appconfig-environment-description

Memeriksa apakah AWS AppConfig lingkungan memiliki deskripsi. Aturannya adalah NON_COMPLIANT jika Configuration.description tidak ada atau string kosong.

Pengidentifikasi: APPCONFIG_ENVIRONMENT_DESCRIPTION

Jenis Sumber Daya: AWS::AppConfig::Environment

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Eropa (Zurich) Wilayah

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

appconfig-environment-tagged

Memeriksa apakah AWS AppConfig lingkungan memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk diperiksa aturan. Aturannya adalah NON_COMPLIANT jika tidak ada tag

atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: APPCONFIG_ENVIRONMENT_TAGGED

Jenis Sumber Daya: AWS::AppConfig::Environment

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Eropa (Zurich) Wilayah

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

appconfig-extension-association-tagged

Memeriksa apakah asosiasi AWS AppConfig ekstensi memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: APPCONFIG_EXTENSION_ASSOCIATION_TAGGED

Jenis Sumber Daya: AWS::AppConfig::ExtensionAssociation

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Tiongkok (Ningxia) Wilayah

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

appconfig-freeform-profile-config-penyimpanan

Memeriksa apakah profil konfigurasi bentuk bebas untuk AWS AppConfig menyimpan data konfigurasi mereka di AWS Secrets Manager atau penyimpanan konfigurasi yang AWS AppConfig dihosting. Aturannya adalah NON_COMPLIANT jika konfigurasi. LocationUri bukan secretsmanager atau dihosting.

Pengidentifikasi: APPCONFIG_FREEFORM_PROFILE_CONFIG_STORAGE

Jenis Sumber Daya: AWS::AppConfig::ConfigurationProfile

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Eropa (Zurich) Wilayah

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

appconfig-hosted-configuration-version-deskripsi

Memeriksa apakah versi konfigurasi yang AWS AppConfig di-host memiliki deskripsi. Aturannya adalah NON_COMPLIANT jika Configuration.description tidak ada atau string kosong.

Pengidentifikasi: APPCONFIG_HOSTED_CONFIGURATION_VERSION_DESCRIPTION

Jenis Sumber Daya: AWS::AppConfig::HostedConfigurationVersion

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Eropa (Zurich) Wilayah

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

appflow-flow-tagged

Memeriksa apakah AppFlow aliran Amazon memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: APPFLOW_FLOW_TAGGED

Jenis Sumber Daya: AWS::AppFlow::Flow

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Asia Pasifik (Mumbai), Eropa (Paris), AS Timur (Ohio), Afrika (Cape Town), Eropa (Irlandia), Eropa (Frankfurt), Amerika Selatan (Sao Paulo), AS Timur (Virginia N.), Asia Pasifik (Seoul), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), AS Barat (California N.), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Wilayah Kanada (Tengah)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

appintegrations-event-integration-description

Memeriksa apakah integrasi AppIntegrations acara Amazon memiliki deskripsi. Aturannya adalah NON_COMPLIANT jika Configuration.description tidak ada.

Pengidentifikasi: APPINTEGRATIONS_EVENT_INTEGRATION_DESCRIPTION

Jenis Sumber Daya: AWS::AppIntegrations::EventIntegration

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Afrika (Cape Town), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Seoul), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Wilayah Kanada (Tengah)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

appintegrations-event-integration-tagged

Memeriksa apakah integrasi AppIntegrations acara Amazon memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: APPINTEGRATIONS_EVENT_INTEGRATION_TAGGED

Jenis Sumber Daya: AWS::AppIntegrations::EventIntegration

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Afrika (Cape Town), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Seoul), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Wilayah Kanada (Tengah)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

appmesh-gateway-route-tagged

Memeriksa apakah rute gateway AWS App Mesh memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk aturan tersebut. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: APPMESH_GATEWAY_ROUTE_TAGGED

Jenis Sumber Daya: AWS::AppMesh::GatewayRoute

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

appmesh-mesh-deny-tcp-penerusan

Memeriksa apakah proxy untuk mesh layanan AWS App Mesh tidak meneruskan lalu lintas TCP secara langsung ke layanan yang tidak digunakan dengan proxy yang ditentukan di mesh. Aturannya adalah NON_COMPLIANT jika Configuration.spec. EgressFilter.Type diatur ke 'ALLOW_ALL'.

Pengidentifikasi: APPMESH_MESH_DENY_TCP_FORWARDING

Jenis Sumber Daya: AWS::AppMesh::Mesh

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

appmesh-mesh-tagged

Memeriksa apakah mesh AWS App Mesh memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk diperiksa aturan. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: APPMESH_MESH_TAGGED

Jenis Sumber Daya: AWS::AppMesh::Mesh

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

appmesh-route-tagged

Memeriksa apakah rute AWS App Mesh memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk diperiksa aturan. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: APPMESH_ROUTE_TAGGED

Jenis Sumber Daya: AWS::AppMesh::Route

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

appmesh-virtual-gateway-backend-default-tls

Memeriksa apakah default backend untuk gateway virtual App AWS Mesh memerlukan gateway virtual untuk berkomunikasi dengan semua port menggunakan TLS. Aturannya adalah NON_COMPLIANT jika Configuration.spec. BackendDefaults. ClientPolicy.Tls.Enforce salah.

Pengidentifikasi: APPMESH_VIRTUAL_GATEWAY_BACKEND_DEFAULTS_TLS

Jenis Sumber Daya: AWS::AppMesh::VirtualGateway

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

appmesh-virtual-gateway-logging-file-path-exists

Memeriksa apakah gateway virtual AWS App Mesh memiliki jalur file untuk menulis log akses ke. Aturannya adalah NON_COMPLIANT jika Configuration.spec.logging. AccessLog.File.Path tidak ada.

Pengidentifikasi: APPMESH_VIRTUAL_GATEWAY_LOGGING_FILE_PATH_EXISTS

Jenis Sumber Daya: AWS::AppMesh::VirtualGateway

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

appmesh-virtual-gateway-tagged

Memeriksa apakah gateway virtual AWS App Mesh memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk aturan tersebut. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: APPMESH_VIRTUAL_GATEWAY_TAGGED

Jenis Sumber Daya: AWS::AppMesh::VirtualGateway

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

appmesh-virtual-node-backend-defaults-tls-on

Memeriksa apakah default backend untuk node virtual App AWS Mesh memerlukan node virtual untuk berkomunikasi dengan semua port menggunakan TLS. Aturannya adalah NON_COMPLIANT jika Configuration.spec. BackendDefaults. ClientPolicy.Tls.Enforce salah.

Pengidentifikasi: APPMESH_VIRTUAL_NODE_BACKEND_DEFAULTS_TLS_ON

Jenis Sumber Daya: AWS::AppMesh::VirtualNode

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

appmesh-virtual-node-logging-file-path-exists

Memeriksa apakah node virtual AWS App Mesh memiliki jalur file untuk menulis log akses ke. Aturannya adalah NON_COMPLIANT jika Configuration.spec.logging. AccessLog.File.Path tidak ada.

Pengidentifikasi: APPMESH_VIRTUAL_NODE_LOGGING_FILE_PATH_EXISTS

Jenis Sumber Daya: AWS::AppMesh::VirtualNode

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

appmesh-virtual-node-tagged

Memeriksa apakah node virtual AWS App Mesh memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk diperiksa aturan. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: APPMESH_VIRTUAL_NODE_TAGGED

Jenis Sumber Daya: AWS::AppMesh::VirtualNode

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

appmesh-virtual-router-tagged

Memeriksa apakah router virtual AWS App Mesh memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk aturan tersebut. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: APPMESH_VIRTUAL_ROUTER_TAGGED

Jenis Sumber Daya: AWS::AppMesh::VirtualRouter

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

appmesh-virtual-service-tagged

Memeriksa apakah layanan virtual AWS App Mesh memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk aturan tersebut. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: APPMESH_VIRTUAL_SERVICE_TAGGED

Jenis Sumber Daya: AWS::AppMesh::VirtualService

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

approved-amis-by-id

Memeriksa apakah EC2 instance menggunakan Amazon Machine Images (AMIs) yang ditentukan. Tentukan daftar AMI yang disetujui IDs. Menjalankan instance dengan AMIs yang tidak ada dalam daftar ini adalah NON_COMPLIANT.

Pengidentifikasi: APPROVED_AMIS_BY_ID

Jenis Sumber Daya: AWS::EC2::Instance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

amiIds, Jenis: CSV

Daftar terpisah koma hingga 21 AMI. IDs Ada batas 1024 karakter.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

approved-amis-by-tag

Memeriksa apakah EC2 instance menggunakan Amazon Machine Images (AMIs) yang ditentukan. Tentukan tag yang mengidentifikasi AMIs. Menjalankan instance dengan AMIs itu tidak memiliki setidaknya satu dari tag yang ditentukan adalah NON_COMPLIANT.

Pengidentifikasi: APPROVED_AMIS_BY_TAG

Jenis Sumber Daya: AWS::EC2::Instance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

amisByTagKeyAndValue, Jenis: StringMap, Default: tag-key:tag-value, other-tag-key

Daftar yang dipisahkan koma hingga 10 AMIs tag (tag-key:tag-value). Misalnya, tag-key1 cocok AMIs dengan tag-key1; tag-key2:value2 cocok dengan tag-key2 dengan nilai 2.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

apprunner-service-in-vpc

Memeriksa apakah layanan AWS App Runner merutekan lalu lintas keluar melalui VPC khusus. Aturannya adalah NON_COMPLIANT jika konfigurasi. NetworkConfiguration. EgressConfiguration. EgressType sama dengan DEFAULT.

Pengidentifikasi: APPRUNNER_SERVICE_IN_VPC

Jenis Sumber Daya: AWS::AppRunner::Service

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Asia Pasifik (Mumbai), Eropa (Paris), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Wilayah Asia Pasifik (Sydney)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

apprunner-service-no-public-akses

Memeriksa apakah AWS AppRunner Layanan tidak dapat diakses publik. Aturannya adalah NON_COMPLIANT jika service.configuration. NetworkConfiguration. IngressConfiguration. IsPubliclyAccessible adalah palsu.

Pengidentifikasi: APPRUNNER_SERVICE_NO_PUBLIC_ACCESS

Jenis Sumber Daya: AWS::AppRunner::Service

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Asia Pasifik (Mumbai), Eropa (Paris), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Wilayah Asia Pasifik (Sydney)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

apprunner-service-observability-enabled

Memeriksa apakah layanan AWS App Runner mengaktifkan observabilitas. Aturannya adalah NON_COMPLIANT jika konfigurasi. ObservabilityConfiguration. ObservabilityEnabled adalah palsu.”

Pengidentifikasi: APPRUNNER_SERVICE_OBSERVABILITY_ENABLED

Jenis Sumber Daya: AWS::AppRunner::Service

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Asia Pasifik (Mumbai), Eropa (Paris), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Wilayah Asia Pasifik (Sydney)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

apprunner-service-tagged

Memeriksa apakah layanan AWS App Runner memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: APPRUNNER_SERVICE_TAGGED

Jenis Sumber Daya: AWS::AppRunner::Service

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Asia Pasifik (Mumbai), Eropa (Paris), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Wilayah Asia Pasifik (Sydney)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

apprunner-vpc-connector-tagged

Memeriksa apakah konektor VPC AWS App Runner memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: APPRUNNER_VPC_CONNECTOR_TAGGED

Jenis Sumber Daya: AWS::AppRunner::VpcConnector

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Asia Pasifik (Mumbai), Eropa (Paris), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Wilayah Asia Pasifik (Sydney)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

appstream-fleet-in-vpc

Memeriksa apakah armada Amazon AppStream 2.0 menggunakan Amazon Virtual Private Cloud (Amazon VPC). Aturannya adalah NON_COMPLIANT jika konfigurasi. VpcConfig tidak ada. Aturannya tidak memeriksa armada elastis.

Pengidentifikasi: APPSTREAM_FLEET_IN_VPC

Jenis Sumber Daya: AWS::AppStream::Fleet

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Asia Pasifik (Mumbai), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Seoul), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Wilayah Kanada (Tengah)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

appsync-associated-with-waf

Memeriksa AWS AppSync APIs apakah terkait dengan daftar kontrol akses AWS WAFv2 web (ACLs). Aturannya adalah NON_COMPLIANT untuk AWS AppSync API jika tidak terkait dengan ACL web.

Pengidentifikasi: APPSYNC_ASSOCIATED_WITH_WAF

Jenis Sumber Daya: AWS::AppSync::GraphQLApi

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Afrika (Cape Town), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur), AWS GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

wafWebAclARNs (Opsional), Jenis: CSV

Daftar Nama Sumber Daya Amazon (ARNs) yang dipisahkan koma untuk web resmi. ACLs

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

appsync-authorization-check

Memeriksa apakah AWS AppSync API menggunakan mekanisme otorisasi yang diizinkan. Aturannya adalah NON_COMPLIANT jika mekanisme otorisasi yang tidak disetujui sedang digunakan.

Pengidentifikasi: APPSYNC_AUTHORIZATION_CHECK

Jenis Sumber Daya: AWS::AppSync::GraphQLApi

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur), AWS GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary) Wilayah

Parameter:

AllowedAuthorizationTypes, Jenis: CSV

Daftar mekanisme AWS AppSync otorisasi yang diizinkan dipisahkan koma. Nilai yang diizinkan adalah: '', 'AWS_LAMBDA',API_KEY' _IAM', 'OPENID_CONNECT',AWS'AMAZON_COGNITO_USER_POOLS'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

appsync-cache-ct-encryption-saat istirahat

Memeriksa apakah cache AWS AppSync API mengaktifkan enkripsi saat istirahat. Aturan ini adalah NON_COMPLIANT jika 'AtRestEncryptionEnabled' salah.

Pengidentifikasi: APPSYNC_CACHE_CT_ENCRYPTION_AT_REST

Jenis Sumber Daya: AWS::AppSync::ApiCache

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Timur Tengah (Bahrain), Eropa (Frankfurt), Amerika Selatan (Sao Paulo), Wilayah AS Timur (Virginia N.)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

appsync-cache-ct-encryption-dalam transit

Memeriksa apakah cache AWS AppSync API mengaktifkan enkripsi saat transit. Aturannya adalah NON_COMPLIANT jika 'TransitEncryptionEnabled' salah.

Pengidentifikasi: APPSYNC_CACHE_CT_ENCRYPTION_IN_TRANSIT

Jenis Sumber Daya: AWS::AppSync::ApiCache

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Timur Tengah (Bahrain), Eropa (Frankfurt), Amerika Selatan (Sao Paulo), Wilayah AS Timur (Virginia N.)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

appsync-cache-encryption-at-istirahat

Memeriksa apakah cache AWS AppSync API mengaktifkan enkripsi saat istirahat. Aturan ini adalah NON_COMPLIANT jika 'AtRestEncryptionEnabled' salah.

Pengidentifikasi: APPSYNC_CACHE_ENCRYPTION_AT_REST

Jenis Sumber Daya: AWS::AppSync::GraphQLApi

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Afrika (Cape Town), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

appsync-logging-enabled

Memeriksa apakah AWS AppSync API telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan, atau jika level logging bidang untuk AWS AppSync API tidak cocok dengan nilai yang ditentukan dalam parameter aturan `fieldLoggingLevel` ".

Pengidentifikasi: APPSYNC_LOGGING_ENABLED

Jenis Sumber Daya: AWS::AppSync::GraphQLApi

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur), AWS GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary) Wilayah

Parameter:

fieldLoggingLevel (Opsional), Jenis: CSV

> Daftar tingkat logging bidang yang dipisahkan koma untuk diperiksa aturan. Misalnya, “ERROR, INFO”.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

athena-data-catalog-description

Memeriksa apakah katalog data Amazon Athena memiliki deskripsi. Aturannya adalah NON_COMPLIANT jika Configuration.description tidak ada.

Pengidentifikasi: ATHENA_DATA_CATALOG_DESCRIPTION

Jenis Sumber Daya: AWS::Athena::DataCatalog

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

athena-prepared-statement-description

Memeriksa apakah Amazon Athena menyiapkan pernyataan memiliki deskripsi. Aturannya adalah NON_COMPLIANT jika Configuration.description tidak ada.

Pengidentifikasi: ATHENA_PREPARED_STATEMENT_DESCRIPTION

Jenis Sumber Daya: AWS::Athena::PreparedStatement

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Eropa (Milan), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Tiongkok (Ningxia) Wilayah

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

athena-workgroup-description

Memeriksa apakah kelompok kerja Amazon Athena memiliki deskripsi. Aturannya adalah NON_COMPLIANT jika Configuration.description tidak ada atau string kosong.

Pengidentifikasi: ATHENA_WORKGROUP_DESCRIPTION

Jenis Sumber Daya: AWS::Athena::WorkGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

athena-workgroup-encrypted-at-istirahat

Memeriksa apakah workgroup Amazon Athena dienkripsi saat istirahat. Aturannya adalah NON_COMPLIANT jika enkripsi data saat istirahat tidak diaktifkan untuk workgroup Athena.

Pengidentifikasi: ATHENA_WORKGROUP_ENCRYPTED_AT_REST

Jenis Sumber Daya: AWS::Athena::WorkGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur), AWS GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Eropa (Zurich) Wilayah

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

athena-workgroup-enforce-workgroup-konfigurasi

Memeriksa apakah grup kerja Amazon Athena yang menggunakan mesin Athena memberlakukan konfigurasi grup kerja untuk mengganti setelan sisi klien. Aturannya adalah NON_COMPLIANT jika konfigurasi. WorkGroupConfiguration. EnforceWorkGroupConfiguration adalah palsu.

Pengidentifikasi: ATHENA_WORKGROUP_ENFORCE_WORKGROUP_CONFIGURATION

Jenis Sumber Daya: AWS::Athena::WorkGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

athena-workgroup-engine-version-upgrade otomatis

Memeriksa apakah grup kerja Amazon Athena yang menggunakan mesin Athena dikonfigurasi untuk meningkatkan secara otomatis. Aturannya adalah NON_COMPLIANT jika konfigurasi. WorkGroupConfiguration. EngineVersion. SelectedEngineVersion bukan 'AUTO'.

Pengidentifikasi: ATHENA_WORKGROUP_ENGINE_VERSION_AUTO_UPGRADE

Jenis Sumber Daya: AWS::Athena::WorkGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

athena-workgroup-logging-enabled

Memeriksa apakah Amazon Athena WorkGroup menerbitkan metrik penggunaan ke Amazon. CloudWatch Aturannya adalah NON_COMPLIANT jika Amazon Athena WorkGroup 'PublishCloudWatchMetricsEnabled' disetel ke false.

Pengidentifikasi: ATHENA_WORKGROUP_LOGGING_ENABLED

Jenis Sumber Daya: AWS::Athena::WorkGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

aurora-last-backup-recovery-point-dibuat

Memeriksa apakah titik pemulihan dibuat untuk cluster Amazon Aurora DB. Aturannya adalah NON_COMPLIANT jika Cluster DB Amazon Relational Database Service (Amazon RDS) tidak memiliki titik pemulihan yang sesuai yang dibuat dalam periode waktu yang ditentukan.

Pengidentifikasi: AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED

Jenis Sumber Daya: AWS::RDS::DBCluster

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

ResourceTags (Opsional), Tipe: String

Tag cluster Aurora DB untuk aturan yang akan diperiksa, dalam format JSON. `{"tagkey" : "tagValue"}`

ResourceID (Opsional), Tipe: String

ID klaster Aurora DB untuk diperiksa aturan.

recoveryPointAgeNilai (Opsional), Jenis: int, Default: 1

Nilai numerik untuk usia maksimum yang diizinkan. Tidak lebih dari 744 jam, 31 untuk hari.

recoveryPointAgeUnit (Opsional), Tipe: String, Default: hari

Satuan waktu untuk usia maksimum yang diizinkan. Nilai yang diterima: 'jam', 'hari'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

aurora-meets-restore-time-target

Memeriksa apakah waktu pemulihan klaster Amazon Aurora DB memenuhi durasi yang ditentukan. Aturannya adalah NON_COMPLIANT jika dari LatestRestoreExecutionTimeMinutes Aurora DB Cluster lebih besar dari menit. maxRestoreTime

Pengidentifikasi: AURORA_MEETS_RESTORE_TIME_TARGET

Jenis Sumber Daya: AWS::RDS::DBCluster

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

maxRestoreTime, Jenis: int

Nilai numerik untuk runtime pemulihan maksimum yang diizinkan.

ResourceTags (Opsional), Tipe: String

Tag cluster Aurora DB untuk aturan yang akan diperiksa, dalam format JSON.

ResourceID (Opsional), Tipe: String

ID cluster Aurora DB untuk aturan yang akan diperiksa.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

aurora-mysql-backtracking-enabled

Memeriksa apakah kluster MySQL Amazon Aurora telah mengaktifkan backtracking. Aturannya adalah NON_COMPLIANT jika cluster Aurora menggunakan MySQL dan tidak mengaktifkan backtracking.

Pengidentifikasi: AURORA_MYSQL_BACKTRACKING_ENABLED

Jenis Sumber Daya: AWS::RDS::DBCluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Eropa (Stockholm), Timur Tengah (Bahrain), Tiongkok (Beijing), Asia Pasifik (Jakarta), Afrika (Cape Town), Timur Tengah (UEA), Amerika Selatan (Sao Paulo), Asia Pasifik (Hong Kong), Asia Pasifik (Hyderabad), Asia Pasifik (Melbourne), Eropa (Milan), (AS-Timur), (AS-Barat) AWS GovCloud , Israel (Tel Aviv) AWS GovCloud , Kanada Barat (Calgary), Wilayah Eropa (Spanyol)

Parameter:

BacktrackWindowInHours (Opsional), Tipe: ganda

Jumlah waktu dalam jam (hingga 72) untuk mundur cluster Aurora MySQL Anda.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

aurora-mysql-cluster-audit-logging

Memeriksa apakah kluster DB MySQL Amazon Aurora mengaktifkan pencatatan audit. Aturannya adalah NON_COMPLIANT jika cluster DB tidak mengaktifkan audit logging.

Pengidentifikasi: AURORA_MYSQL_CLUSTER_AUDIT_LOGGING

Jenis Sumber Daya: AWS::RDS::DBCluster

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (Bahrain), Tiongkok (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

aurora-resources-in-logically-air-gapped-vault

Memeriksa apakah cluster Amazon Aurora DB berada dalam lemari besi yang memiliki jarak udara secara logis. Aturannya adalah NON_COMPLIANT jika klaster DB Amazon Aurora tidak berada dalam brankas yang memiliki gap udara secara logis dalam periode waktu yang ditentukan.

Pengidentifikasi: AURORA_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

Jenis Sumber Daya: AWS::RDS::DBCluster

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

ResourceTags (Opsional), Tipe: String

Tag cluster Aurora DB untuk aturan yang akan diperiksa, dalam format JSON.

ResourceID (Opsional), Tipe: String

ID cluster Aurora DB untuk aturan yang akan diperiksa.

recoveryPointAgeNilai (Opsional), Jenis: int, Default: 1

Nilai numerik untuk usia maksimum yang diizinkan. Tidak lebih dari 2184 jam, 91 untuk hari.

recoveryPointAgeUnit (Opsional), Tipe: String, Default: hari

Satuan waktu untuk usia maksimum yang diizinkan. Nilai yang diterima: 'jam', 'hari'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

aurora-resources-protected-by-rencana cadangan

Memeriksa apakah cluster Amazon Aurora DB dilindungi oleh paket cadangan. Aturannya adalah NON_COMPLIANT jika Cluster Database Amazon Relational Database Service (Amazon RDS) tidak dilindungi oleh paket cadangan.

Pengidentifikasi: AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Jenis Sumber Daya: AWS::RDS::DBCluster

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

ResourceTags (Opsional), Tipe: String

Tag cluster Aurora DB untuk aturan yang akan diperiksa, dalam format JSON. `{"tagkey" : "tagValue"}`

ResourceID (Opsional), Tipe: String

ID klaster Aurora DB untuk diperiksa aturan.

crossRegionList (Opsional), Tipe: String

Daftar wilayah tujuan yang dipisahkan koma untuk salinan cadangan lintas wilayah yang akan disimpan

crossAccountList (Opsional), Tipe: String

Daftar akun tujuan yang dipisahkan koma untuk salinan cadangan lintas akun yang akan disimpan

maxRetentionDays (Opsional), Jenis: int

Periode retensi maksimum dalam beberapa hari untuk Backup Vault Lock

minRetentionDays (Opsional), Jenis: int

Periode retensi minimum dalam beberapa hari untuk Backup Vault Lock

backupVaultLockPeriksa (Opsional), Tipe: String

Nilai yang diterima: 'Benar' atau 'False'. Masukkan 'Benar' untuk aturan untuk memeriksa apakah sumber daya dicadangkan di brankas yang terkunci

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

autoscaling-capacity-rebalancing

Memeriksa apakah Penyeimbangan Kembali Kapasitas diaktifkan untuk grup Auto EC2 Scaling Amazon yang menggunakan beberapa jenis instans. Aturannya adalah NON_COMPLIANT jika Rebalancing kapasitas tidak diaktifkan.

Pengidentifikasi: AUTOSCALING_CAPACITY_REBALANCING

Jenis Sumber Daya: AWS::AutoScaling::AutoScalingGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

autoscaling-group-elb-healthcheck-diperlukan

Memeriksa apakah grup Amazon EC2 Auto Scaling yang terkait dengan Elastic Load Balancer menggunakan pemeriksaan kesehatan Elastic Load Balancing. Aturannya adalah NON_COMPLIANT jika grup EC2 Auto Scaling Amazon tidak menggunakan pemeriksaan kesehatan Elastic Load Balancing.

Pengidentifikasi: AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED

Jenis Sumber Daya: AWS::AutoScaling::AutoScalingGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Timur Tengah (UEA), Asia Pasifik (Taipei)

Parameter:

Tidak ada

Evaluasi Proaktif

Untuk langkah-langkah tentang cara menjalankan aturan ini dalam mode proaktif, lihat Mengevaluasi Sumber Daya Anda dengan AWS Config Aturan. Agar aturan ini mengembalikan COMPLIANT

dalam mode proaktif, skema konfigurasi sumber daya untuk StartResourceEvaluationAPI harus menyertakan input berikut, yang dikodekan sebagai string:

```
"ResourceConfiguration":
...
{
   "LoadBalancerNames": "[my-load-balancer-1, my-load-balancer-2, my-load-
balancer-3, ...]",
   "HealthCheckType": HealthCheckType*"
}
...
```

* Nilai yang valid adalah `EC2` (default),`ELB`, dan`VPC_LATTICE`. Jenis pemeriksaan `VPC_LATTICE` kesehatan dicadangkan untuk digunakan dengan VPC Lattice, yang dalam rilis pratinjau dan dapat berubah sewaktu-waktu. Untuk informasi selengkapnya, lihat Pemeriksaan Kesehatan untuk instans Auto Scaling di Panduan Pengguna Amazon EC2 Auto Scaling.

Untuk informasi lebih lanjut tentang evaluasi proaktif, lihat Mode Evaluasi.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

autoscaling-launchconfig-requires-imdsv2

Memeriksa IMDSv2 apakah hanya diaktifkan. Aturan ini NON_COMPLIANT jika versi Metadata tidak disertakan dalam konfigurasi peluncuran atau jika kedua Metadata V1 dan V2 diaktifkan.

Pengidentifikasi: AUTOSCALING_LAUNCHCONFIG_REQUIRES_ IMDSV2

Jenis Sumber Daya: AWS::AutoScaling::LaunchConfiguration

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

autoscaling-launch-config-hop-batas

Memeriksa jumlah hop jaringan yang dapat dilakukan oleh token metadata. Aturan ini NON_COMPLIANT jika batas hop respons Metadata lebih besar dari 1.

Pengidentifikasi: AUTOSCALING_LAUNCH_CONFIG_HOP_LIMIT

Jenis Sumber Daya: AWS::AutoScaling::LaunchConfiguration

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Asia Pasifik (Malaysia), AWS GovCloud (AS-Timur), AWS GovCloud (AS-Barat), Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

autoscaling-launch-config-public-ip-dinonaktifkan

Memeriksa apakah grup EC2 Auto Scaling Amazon mengaktifkan alamat IP publik melalui Konfigurasi Peluncuran. Aturannya adalah NON_COMPLIANT jika Konfigurasi Peluncuran untuk grup EC2 Auto Scaling Amazon telah disetel ke 'benar'. AssociatePublicIpAddress

Pengidentifikasi: AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED

Jenis Sumber Daya: AWS::AutoScaling::LaunchConfiguration

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

autoscaling-launch-template

Memeriksa apakah grup Auto Scaling Amazon Elastic Compute Cloud (EC2) dibuat dari template peluncuran EC2 . Aturannya adalah NON_COMPLIANT jika grup penskalaan tidak dibuat dari template peluncuran. EC2

Pengidentifikasi: AUTOSCALING_LAUNCH_TEMPLATE

Jenis Sumber Daya: AWS::AutoScaling::AutoScalingGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), AWS GovCloud (AS-Timur), AWS GovCloud (AS-Barat), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

autoscaling-multiple-az

Memeriksa apakah grup Auto Scaling mencakup beberapa Availability Zone. Aturannya adalah NON_COMPLIANT jika grup Auto Scaling tidak menjangkau beberapa Availability Zone.

Pengidentifikasi: AUTOSCALING_MULTIPLE_AZ

Jenis Sumber Daya: AWS::AutoScaling::AutoScalingGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), AWS GovCloud (AS-Timur), AWS GovCloud (AS-Barat), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

minAvailabilityZones (Opsional), Jenis: int

Jumlah minimum zona Ketersediaan yang diharapkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

autoscaling-multiple-instance-types

Memeriksa apakah grup EC2 Auto Scaling Amazon menggunakan beberapa jenis instans. Aturannya adalah NON_COMPLIANT jika grup EC2 Auto Scaling Amazon hanya memiliki satu jenis instance yang ditentukan. Aturan ini tidak mengevaluasi tipe instance berbasis atribut.

Pengidentifikasi: AUTOSCALING_MULTIPLE_INSTANCE_TYPES

Jenis Sumber Daya: AWS::AutoScaling::AutoScalingGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

backup-plan-min-frequency-and-min-retention-check

Memeriksa apakah rencana cadangan memiliki aturan cadangan yang memenuhi frekuensi dan periode retensi yang diperlukan. Aturannya adalah NON_COMPLIANT jika titik pemulihan tidak dibuat setidaknya sesering frekuensi yang ditentukan atau kedaluwarsa sebelum periode yang ditentukan.

Pengidentifikasi: BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK

Jenis Sumber Daya: AWS::Backup::BackupPlan

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

requiredFrequencyValue (Opsional), Jenis: int, Default: 1

Nilai numerik untuk frekuensi cadangan yang diperlukan. Maksimal 24 jam, 31 untuk hari.

requiredRetentionDays (Opsional), Jenis: int, Default: 35

Periode retensi yang diperlukan dalam beberapa hari.

requiredFrequencyUnit (Opsional), Tipe: String, Default: hari

Satuan waktu untuk frekuensi cadangan yang diperlukan. Nilai yang diterima: 'jam', 'hari'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

backup-recovery-point-encrypted

Memeriksa apakah titik pemulihan dienkripsi. Aturannya adalah NON_COMPLIANT jika titik pemulihan tidak dienkripsi.

Pengidentifikasi: BACKUP_RECOVERY_POINT_ENCRYPTED

Jenis Sumber Daya: AWS::Backup::RecoveryPoint

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

backup-recovery-point-manual-penghapusan-dinonaktifkan

Memeriksa apakah brankas cadangan memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Aturannya adalah NON_COMPLIANT jika Brankas Cadangan tidak memiliki kebijakan berbasis sumber daya atau memiliki kebijakan tanpa pernyataan 'Deny' yang sesuai (pernyataan dengan cadangan:DeleteRecoveryPoint, cadangan:, dan cadangan: izin). UpdateRecoveryPointLifecycle PutBackupVaultAccessPolicy

> **Note**
>
> Wildcard diperlukan untuk **`"Resource"`** dan **`"Principal"`** dari pernyataan Deny
> Aturan mensyaratkan bahwa `"Resource"` dan `"Principal"` pernyataan Deny harus memiliki wildcard dalam kebijakan akses vault. Jika tidak, aturan mengembalikan NON_COMPLIANT.

Pengidentifikasi: BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED

Jenis Sumber Daya: AWS::Backup::BackupVault

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

principalArnList (Opsional), Jenis: CSV

Daftar AWS Identitas dan Manajemen Akses (IAM) and Access Management (IAM) Amazon Resource Names ARNs () yang dipisahkan koma agar aturan TIDAK diperiksa.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

backup-recovery-point-minimum-pemeriksaan retensi

Memeriksa apakah titik pemulihan berakhir tidak lebih awal dari setelah periode yang ditentukan. Aturannya adalah NON_COMPLIANT jika titik pemulihan memiliki titik retensi yang kurang dari periode retensi yang diperlukan.

Pengidentifikasi: BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK

Jenis Sumber Daya: AWS::Backup::RecoveryPoint

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

requiredRetentionDays (Opsional), Jenis: int, Default: 35

Periode retensi yang diperlukan dalam beberapa hari.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

batch-compute-environment-enabled

Memeriksa apakah lingkungan komputasi AWS Batch diaktifkan. Aturannya adalah NON_COMPLIANT jika Configuration.state adalah 'DISABLED'.

Pengidentifikasi: BATCH_COMPUTE_ENVIRONMENT_ENABLED

Jenis Sumber Daya: AWS::Batch::ComputeEnvironment

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

batch-compute-environment-managed

Memeriksa apakah lingkungan komputasi AWS Batch dikelola. Aturannya adalah NON_COMPLIANT jika Configuration.type adalah 'UNMANAGED'.

Pengidentifikasi: BATCH_COMPUTE_ENVIRONMENT_MANAGED

Jenis Sumber Daya: AWS::Batch::ComputeEnvironment

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

batch-compute-environment-tagged

Memeriksa apakah lingkungan komputasi AWS Batch memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: BATCH_COMPUTE_ENVIRONMENT_TAGGED

Jenis Sumber Daya: AWS::Batch::ComputeEnvironment

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

batch-job-queue-enabled

Memeriksa apakah antrian pekerjaan AWS Batch diaktifkan. Aturannya adalah NON_COMPLIANT jika Configuration.state adalah 'DISABLED'.

Pengidentifikasi: BATCH_JOB_QUEUE_ENABLED

Jenis Sumber Daya: AWS::Batch::JobQueue

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

batch-job-queue-tagged

Memeriksa apakah antrian pekerjaan AWS Batch memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: BATCH_JOB_QUEUE_TAGGED

Jenis Sumber Daya: AWS::Batch::JobQueue

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

batch-managed-compute-environment-using-launch-template

Memeriksa apakah lingkungan komputasi terkelola AWS Batch dikonfigurasi menggunakan template peluncuran. Aturannya adalah NON_COMPLIANT jika konfigurasi. ComputeResources. LaunchTemplate tidak ada.

Pengidentifikasi: BATCH_MANAGED_COMPUTE_ENVIRONMENT_USING_LAUNCH_TEMPLATE

Jenis Sumber Daya: AWS::Batch::ComputeEnvironment

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

batch-managed-compute-env-compute-resources-tagged

Memeriksa apakah lingkungan komputasi terkelola AWS Batch menghitung sumber daya memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Tag yang dimulai dengan 'aws: 'tidak dicentang.

Pengidentifikasi: BATCH_MANAGED_COMPUTE_ENV_COMPUTE_RESOURCES_TAGGED

Jenis Sumber Daya: AWS::Batch::ComputeEnvironment

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

batch-scheduling-policy-tagged

Memeriksa apakah kebijakan penjadwalan AWS Batch memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: BATCH_SCHEDULING_POLICY_TAGGED

Jenis Sumber Daya: AWS::Batch::SchedulingPolicy

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

beanstalk-enhanced-health-reporting-diaktifkan

Memeriksa apakah lingkungan AWS Elastic Beanstalk dikonfigurasi untuk pelaporan kesehatan yang ditingkatkan. Aturannya SESUAI jika lingkungan dikonfigurasi untuk pelaporan kesehatan yang ditingkatkan. Aturannya adalah NON_COMPLIANT jika lingkungan dikonfigurasi untuk pelaporan kesehatan dasar.

Pengidentifikasi: BEANSTALK_ENHANCED_HEALTH_REPORTING_ENABLED

Jenis Sumber Daya: AWS::ElasticBeanstalk::Environment

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Eropa (Zuryol) lich) Wilayah

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

cassandra-keyspace-tagged

Memeriksa apakah ruang kunci Amazon Keyspaces (untuk Apache Cassandra) memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: CASSANDRA_KEYSPACE_TAGGED

Jenis Sumber Daya: AWS::Cassandra::Keyspace

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Eropa (Stockholm), Timur Tengah (Bahrain), Asia Pasifik (Mumbai), Eropa (Paris), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), Amerika Selatan (Sao Paulo), Asia Pasifik (Hong Kong), AS Timur (Virginia N.), Asia Pasifik (Seoul), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), AS Barat (California N.), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Wilayah Kanada (Tengah)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

clb-desync-mode-check

Memeriksa apakah Classic Load Balancers (CLB) dikonfigurasi dengan mode mitigasi Desync yang ditentukan pengguna. Aturannya adalah NON_COMPLIANT jika mode mitigasi CLB Desync tidak cocok dengan mode mitigasi Desync yang ditentukan pengguna.

Pengidentifikasi: CLB_DESYNC_MODE_CHECK

Jenis Sumber Daya: AWS::ElasticLoadBalancing::LoadBalancer

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

DesyncMode, Jenis: CSV

Daftar nilai yang dipisahkan koma. Anda dapat memilih maksimal dua. Nilai yang valid termasuk 'Defensive', 'Strictest', dan 'Monitor'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

clb-multiple-az

Memeriksa apakah Classic Load Balancer mencakup beberapa Availability Zones (). AZs Aturannya adalah NON_COMPLIANT jika Classic Load Balancer mencakup kurang dari AZs 2 atau tidak mencakup jumlah AZs yang disebutkan dalam `minAvailabilityZones` parameter (jika disediakan).

Pengidentifikasi: CLB_MULTIPLE_AZ

Jenis Sumber Daya: AWS::ElasticLoadBalancing::LoadBalancer

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), AWS GovCloud (AS-Timur), AWS GovCloud (AS-Barat), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

minAvailabilityZones (Opsional), Jenis: int

Jumlah minimum yang diinginkan dari yang diharapkan AZs. Nilai yang valid adalah antara 2 dan 10, keduanya inklusif. Nilai default adalah 2 jika parameter tidak ditentukan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

cloudformation-stack-drift-detection-periksa

Memeriksa apakah konfigurasi sebenarnya dari tumpukan AWS CloudFormation (AWS CloudFormation) berbeda, atau telah melayang, dari konfigurasi yang diharapkan. Tumpukan dianggap telah hanyut jika satu atau lebih sumber dayanya berbeda dari konfigurasi yang diharapkan. Aturan dan tumpukan adalah COMPLIANT ketika status stack drift adalah IN_SYNC. Aturannya adalah NON_COMPLIANT jika status stack drift adalah DRIFTED.

> **Note**
>
> Aturan ini melakukan DetectStackDrift operasi pada setiap tumpukan di akun Anda. DetectStackDrift Operasi dapat memakan waktu hingga beberapa menit, tergantung pada jumlah sumber daya yang terkandung dalam tumpukan. Mengingat bahwa waktu eksekusi maksimum aturan ini dibatasi hingga 15 menit, ada kemungkinan aturan tersebut habis sebelum menyelesaikan evaluasi semua tumpukan di akun Anda.
> Jika Anda mengalami masalah ini, disarankan agar Anda membatasi jumlah tumpukan dalam cakupan aturan, menggunakan tag. Anda dapat melakukan tindakan berikut:
>
> 1. Bagilah tumpukan Anda menjadi beberapa kelompok, masing-masing dengan tag yang berbeda.
> 2. Terapkan tag yang sama ke semua tumpukan di grup itu.
> 3. Memiliki beberapa contoh aturan ini di akun Anda, masing-masing dicakup oleh tag yang berbeda. Ini memungkinkan setiap instance aturan untuk hanya memproses tumpukan yang memiliki tag terkait yang disebutkan dalam cakupannya.

Pengidentifikasi: CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK

Jenis Sumber Daya: AWS::CloudFormation::Stack

Jenis pemicu: Perubahan konfigurasi dan Periodik

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Melbourne), Israel (Tel Aviv), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

cloudformationRoleArn, Tipe: String

Nama Sumber Daya Amazon (ARN) dari peran IAM dengan izin kebijakan untuk mendeteksi penyimpangan tumpukan. AWS CloudFormation Untuk informasi tentang izin IAM yang diperlukan untuk peran tersebut, lihat Mendeteksi perubahan konfigurasi yang tidak dikelola pada tumpukan dan sumber daya | Pertimbangan saat mendeteksi penyimpangan dalam Panduan Pengguna.AWS CloudFormation

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

cloudformation-stack-notification-check

Memeriksa apakah CloudFormation tumpukan Anda mengirim pemberitahuan acara ke topik Amazon SNS. Secara opsional memeriksa apakah topik Amazon SNS yang ditentukan digunakan. Aturannya adalah NON_COMPLIANT jika CloudFormation tumpukan tidak mengirim notifikasi.

Pengidentifikasi: CLOUDFORMATION_STACK_NOTIFICATION_CHECK

Jenis Sumber Daya: AWS::CloudFormation::Stack

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

SNSTOpic1 (Opsional), Tipe: String

SNS Topik ARN.

SNSTOpic2 (Opsional), Tipe: String

SNS Topik ARN.

SNSTOpic3 (Opsional), Tipe: String

SNS Topik ARN.

SNSTOpic4 (Opsional), Tipe: String

SNS Topik ARN.

SNSTOpic5 (Opsional), Tipe: String

SNS Topik ARN.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

cloudfront-accesslogs-enabled

Memeriksa apakah CloudFront distribusi Amazon dikonfigurasi untuk mengirimkan log akses ke bucket Amazon S3 menggunakan pencatatan standar (lama). Aturannya adalah NON_COMPLIANT jika CloudFront distribusi tidak memiliki pencatatan lama yang dikonfigurasi.

Pengidentifikasi: CLOUDFRONT_ACCESSLOGS_ENABLED

Jenis Sumber Daya: AWS::CloudFront::Distribution

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Wilayah AS Timur (Virginia Utara)

Parameter:

S3 BucketName (Opsional), Tipe: String

Nama bucket Amazon S3 untuk menyimpan log akses server.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

cloudfront-associated-with-waf

Memeriksa apakah CloudFront distribusi Amazon dikaitkan dengan firewall aplikasi web (WAF) atau daftar kontrol akses WAFv2 web (ACLs). Aturannya adalah NON_COMPLIANT jika CloudFront distribusi tidak terkait dengan ACL web WAF.

Pengidentifikasi: CLOUDFRONT_ASSOCIATED_WITH_WAF

Jenis Sumber Daya: AWS::CloudFront::Distribution

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Wilayah AS Timur (Virginia Utara)

Parameter:

wafWebAclIds (Opsional), Jenis: CSV

> Daftar ACL web yang dipisahkan koma IDs untuk WAF atau web ACL Amazon Resource Names () untuk. ARNs WAFV2

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

cloudfront-custom-ssl-certificate

Memeriksa apakah sertifikat yang terkait dengan CloudFront distribusi Amazon adalah sertifikat Secure Sockets Layer (SSL) default.

Pengidentifikasi: CLOUDFRONT_CUSTOM_SSL_CERTIFICATE

Jenis Sumber Daya: AWS::CloudFront::Distribution

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Wilayah AS Timur (Virginia Utara)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

cloudfront-default-root-object-dikonfigurasi

Memeriksa apakah CloudFront distribusi Amazon dikonfigurasi untuk mengembalikan objek tertentu yang merupakan objek root default.

Pengidentifikasi: CLOUDFRONT_DEFAULT_ROOT_OBJECT_CONFIGURATED

Jenis Sumber Daya: AWS::CloudFront::Distribution

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Wilayah AS Timur (Virginia Utara)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

cloudfront-no-deprecated-ssl-protokol

Memeriksa apakah CloudFront distribusi menggunakan protokol SSL yang tidak digunakan lagi untuk komunikasi HTTPS antara lokasi tepi dan asal kustom. CloudFront Aturan ini adalah NON_COMPLIANT untuk CloudFront distribusi jika ada '' termasuk 'OriginSslProtocols'. SSLv3

Pengidentifikasi: CLOUDFRONT_NO_DEPRECATED_SSL_PROTOCOLS

Jenis Sumber Daya: AWS::CloudFront::Distribution

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Wilayah AS Timur (Virginia Utara)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

cloudfront-origin-access-identity-diaktifkan

Memeriksa apakah CloudFront distribusi dengan tipe Asal Amazon S3 memiliki identitas akses asal yang dikonfigurasi. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi didukung oleh S3 dan jenis asal apa pun tidak dikonfigurasi OAI, atau asalnya bukan bucket S3.

> **Note**
>
> Aturan tidak kembali `NOT_APPLICABLE` jika asalnya bukan ember S3.

Pengidentifikasi: CLOUDFRONT_ORIGIN_ACCESS_IDENTITY_ENABLED

Jenis Sumber Daya: AWS::CloudFront::Distribution

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Wilayah AS Timur (Virginia Utara)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

cloudfront-origin-failover-enabled

Memeriksa apakah CloudFront distribusi Amazon dikonfigurasi dengan setidaknya 2 asal dalam grup asal.

Pengidentifikasi: CLOUDFRONT_ORIGIN_FAILOVER_ENABLED

Jenis Sumber Daya: AWS::CloudFront::Distribution

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Wilayah AS Timur (Virginia Utara)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

cloudfront-s3- origin-access-control-enabled

Memeriksa apakah CloudFront distribusi Amazon dengan jenis Asal Simple Storage Service (Amazon S3) Amazon S3 mengaktifkan kontrol akses asal (OAC). Aturannya adalah NON_COMPLIANT untuk CloudFront distribusi dengan asal Amazon S3 yang tidak mengaktifkan OAC.

Pengidentifikasi: CLOUDFRONT_S3_ORIGIN_ACCESS_CONTROL_ENABLED

Jenis Sumber Daya: AWS::CloudFront::Distribution

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Wilayah AS Timur (Virginia Utara)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

cloudfront-s3- origin-non-existent-bucket

Memeriksa apakah CloudFront distribusi Amazon mengarah ke bucket S3 yang tidak ada. Aturannya adalah NON_COMPLIANT jika `S3 OriginConfig `untuk CloudFront distribusi menunjuk ke bucket S3 yang tidak ada. Aturan tidak mengevaluasi bucket S3 dengan hosting situs web statis.

Pengidentifikasi: CLOUDFRONT_S3_ORIGIN_NON_EXISTENT_BUCKET

Jenis Sumber Daya: AWS::CloudFront::Distribution

Jenis pemicu: Berkala

Wilayah AWS: Hanya tersedia di China (Beijing), Wilayah AS Timur (Virginia N.)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

cloudfront-security-policy-check

Memeriksa apakah CloudFront distribusi Amazon menggunakan kebijakan keamanan minimum dan rangkaian sandi TLSv1 0,2 atau lebih tinggi untuk koneksi penampil. Aturan ini adalah NON_COMPLIANT untuk CloudFront distribusi jika di bawah .2_2018 minimumProtocolVersion . TLSv1

Pengidentifikasi: CLOUDFRONT_SECURITY_POLICY_CHECK

Jenis Sumber Daya: AWS::CloudFront::Distribution

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Wilayah AS Timur (Virginia Utara)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

cloudfront-sni-enabled

Aturan ini akan memeriksa apakah CloudFront distribusi dikonfigurasi untuk menggunakan SNI untuk melayani permintaan HTTPS.

Pengidentifikasi: CLOUDFRONT_SNI_ENABLED

Jenis Sumber Daya: AWS::CloudFront::Distribution

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Wilayah AS Timur (Virginia Utara)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

cloudfront-ssl-policy-check

Memeriksa apakah CloudFront distribusi Amazon dikonfigurasi dengan kebijakan keamanan yang ditentukan.Aturannya adalah NON_COMPLIANT jika CloudFront Distribusi tidak dikonfigurasi dengan kebijakan keamanan yang Anda tentukan.

Pengidentifikasi: CLOUDFRONT_SSL_POLICY_CHECK

Jenis Sumber Daya: AWS::CloudFront::Distribution

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Wilayah AS Timur (Virginia Utara)

Parameter:

Kebijakan Keamanan, Jenis: CSV

> Daftar kebijakan keamanan CloudFront distribusi yang dipisahkan koma untuk diperiksa aturan. Misalnya: "TLSv1.2_2018, .2_2019, TLSv1 .2_2021". TLSv1 Untuk daftar nilai yang valid, lihat Panduan CloudFront Pengembang Amazon.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

cloudfront-traffic-to-origin-dienkripsi

Memeriksa apakah CloudFront distribusi Amazon mengenkripsi lalu lintas ke asal kustom. Aturannya adalah NON_COMPLIANT jika '' is OriginProtocolPolicy 'http-only' atau jika '' adalah 'match-viewer' dan OriginProtocolPolicy '' adalah 'allow-all'. ViewerProtocolPolicy

Pengidentifikasi: CLOUDFRONT_TRAFFIC_TO_ORIGIN_ENCRYPTED

Jenis Sumber Daya: AWS::CloudFront::Distribution

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Wilayah AS Timur (Virginia Utara)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

cloudfront-viewer-policy-https

Memeriksa apakah CloudFront distribusi Amazon Anda menggunakan HTTPS (secara langsung atau melalui pengalihan). Aturannya adalah NON_COMPLIANT jika nilai ViewerProtocolPolicy disetel ke 'allow-all' untuk atau untuk. DefaultCacheBehavior CacheBehaviors

Pengidentifikasi: CLOUDFRONT_VIEWER_POLICY_HTTPS

Jenis Sumber Daya: AWS::CloudFront::Distribution

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Wilayah AS Timur (Virginia Utara)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

cloudtrail-all-read-s3- data-event-check

Memeriksa apakah jejak AWS CloudTrail Multi-wilayah diaktifkan dan mencatat semua peristiwa data S3 yang telah dibaca untuk bucket Anda. Aturannya adalah NON_COMPLIANT jika tidak ada jejak Multi-wilayah yang mencatat semua tipe peristiwa data S3 baca untuk semua bucket S3 saat ini dan masa depan.

Pengidentifikasi: CLOUDTRAIL_ALL_READ_S3_DATA_EVENT_CHECK

Jenis Sumber Daya: AWS: :::Akun

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

cloudtrail-all-write-s3- data-event-check

Memeriksa apakah jejak AWS CloudTrail Multi-wilayah diaktifkan dan mencatat semua peristiwa data tulis S3 untuk bucket Anda. Aturannya adalah NON_COMPLIANT jika tidak ada jejak Multi-wilayah yang mencatat semua tipe peristiwa data tulis S3 untuk semua bucket S3 saat ini dan masa depan.

Pengidentifikasi: CLOUDTRAIL_ALL_WRITE_S3_DATA_EVENT_CHECK

Jenis Sumber Daya: AWS: :::Akun

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

cloudtrail-s3- bucket-access-logging

Memeriksa apakah konfigurasi bucket S3 untuk AWS CloudTrail log Anda mengaktifkan pencatatan akses server Amazon S3. Aturannya adalah NON_COMPLIANT jika setidaknya satu bucket S3 untuk CloudTrail jejak tidak mengaktifkan logging akses server S3.

Pengidentifikasi: CLOUDTRAIL_S3_BUCKET_ACCESS_LOGGING

Jenis Sumber Daya: AWS::CloudTrail::Trail

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

cloudtrail-s3- bucket-public-access-prohibited

Memeriksa apakah konfigurasi bucket S3 untuk AWS CloudTrail log Anda memblokir akses publik. Aturannya adalah NON_COMPLIANT jika setidaknya satu bucket S3 untuk CloudTrail jejak dapat diakses publik.

Pengidentifikasi: CLOUDTRAIL_S3_BUCKET_PUBLIC_ACCESS_FORBIDNED

Jenis Sumber Daya: AWS::CloudTrail::Trail

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

cloudtrail-s3-dataevents-diaktifkan

Memeriksa apakah setidaknya satu AWS CloudTrail jejak mencatat peristiwa data Amazon Simple Storage Service (Amazon S3) untuk semua bucket S3. Aturannya adalah NON_COMPLIANT jika ada jejak atau jika tidak ada jejak yang merekam peristiwa data S3.

Pengidentifikasi: CLOUDTRAIL_S3_DATAEVENTS_ENABLED

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei)

Parameter:

S3 BucketNames (Opsional), Tipe: String

> Daftar nama bucket S3 yang dipisahkan koma yang mana pencatatan peristiwa datanya harus diaktifkan. Pemeriksaan perilaku default untuk semua bucket S3.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

cloudtrail-security-trail-enabled

Memeriksa bahwa setidaknya ada satu AWS CloudTrail jejak yang ditentukan dengan praktik terbaik keamanan. Aturan ini SESUAI jika setidaknya ada satu jejak yang memenuhi semua hal berikut:

- merekam acara layanan global
- adalah jejak multi-wilayah
- telah mengaktifkan validasi file Log
- dienkripsi dengan kunci KMS
- merekam peristiwa untuk membaca dan menulis
- acara manajemen catatan
- tidak mengecualikan acara manajemen apa pun

Aturan ini NON_COMPLIANT jika tidak ada jejak yang memenuhi semua kriteria yang disebutkan di atas.

Pengidentifikasi: CLOUDTRAIL_SECURITY_TRAIL_ENABLED

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

cloudwatch-alarm-action-check

Memeriksa apakah CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memeriksa apakah ada tindakan yang cocok

dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

Pengidentifikasi: CLOUDWATCH_ALARM_ACTION_CHECK

Jenis Sumber Daya: AWS::CloudWatch::Alarm

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

alarmActionRequired, Tipe: String, Default: betul

Alarm memiliki setidaknya satu tindakan.

insufficientDataActionDiperlukan, Tipe: String, Default: betul

Alarm memiliki setidaknya satu tindakan ketika alarm bertransisi ke status INSUFFICIENT_DATA dari status lain.

okActionRequired, Tipe: String, Bawaan: salah

Alarm memiliki setidaknya satu tindakan ketika alarm bertransisi ke status OK dari keadaan lain.

action1 (Opsional), Tipe: String

Tindakan untuk mengeksekusi, ditentukan sebagai ARN.

action2 (Opsional), Tipe: String

Tindakan untuk mengeksekusi, ditentukan sebagai ARN.

action3 (Opsional), Tipe: String

Tindakan untuk mengeksekusi, ditentukan sebagai ARN.

action4 (Opsional), Tipe: String

Tindakan untuk mengeksekusi, ditentukan sebagai ARN.

tindakan5 (Opsional), Tipe: String

Tindakan untuk mengeksekusi, ditentukan sebagai ARN.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

cloudwatch-alarm-action-enabled-periksa

Memeriksa apakah tindakan CloudWatch alarm Amazon dalam status diaktifkan. Aturannya adalah NON_COMPLIANT jika tindakan CloudWatch alarm tidak dalam status diaktifkan.

Pengidentifikasi: CLOUDWATCH_ALARM_ACTION_ENABLED_CHECK

Jenis Sumber Daya: AWS::CloudWatch::Alarm

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), AWS GovCloud (AS-Timur), AWS GovCloud (AS-Barat), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

cloudwatch-alarm-resource-check

Memeriksa apakah jenis sumber daya memiliki CloudWatch alarm untuk metrik bernama. Untuk jenis sumber daya, Anda dapat menentukan volume EBS, EC2 instans, kluster Amazon RDS, atau bucket S3. Aturannya adalah COMPLIANT jika metrik bernama memiliki ID sumber daya dan CloudWatch alarm.

Pengidentifikasi: CLOUDWATCH_ALARM_RESOURCE_CHECK

Jenis Sumber Daya: AWS::EC2::Instance, AWS::RDS::DBCluster, AWS::S3::Bucket, AWS::EC2::Volume

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

resourceType, Tipe: String

AWS jenis sumber daya. Nilainya dapat berupa salah satu dari yang berikut: AWS::EC2::Volume, AWS::EC2::Instance, AWS::RDS::DBCluster, atau AWS::S3::Bucket.

metricName, Tipe: String

Nama untuk metrik yang terkait dengan alarm (misalnya, 'CPUUtilization' untuk EC2 instance).

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

cloudwatch-alarm-settings-check

Memeriksa apakah CloudWatch alarm dengan nama metrik yang diberikan memiliki pengaturan yang ditentukan.

Pengidentifikasi: CLOUDWATCH_ALARM_SETTINGS_CHECK

Jenis Sumber Daya: AWS::CloudWatch::Alarm

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

metricName, Tipe: String

Nama untuk metrik yang terkait dengan alarm.

ambang batas (Opsional), Jenis: int

Nilai terhadap perbandingan statistik yang ditentukan.

EvaluationPeriod (Opsional), Jenis: int

Jumlah periode yang mana data dibandingkan dengan ambang batas yang ditentukan.

periode (Opsional), Jenis: int, Default: 300

Periode, dalam detik, di mana statistik yang ditentukan diterapkan.

ComparisonOperator (Opsional), Tipe: String

Operasi untuk membandingkan statistik dan ambang batas yang ditentukan (misalnya, 'GreaterThanThreshold').

statistik (Opsional), Tipe: String

Statistik untuk metrik yang terkait dengan alarm (misalnya, 'Rata-rata' atau 'Jumlah').

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

cloudwatch-log-group-encrypted

Memeriksa apakah Grup CloudWatch Log Amazon dienkripsi dengan kunci AWS KMS atau ID kunci AWS KMS tertentu. Aturannya adalah NON_COMPLIANT jika Grup CloudWatch Log tidak dienkripsi dengan kunci KMS atau dienkripsi dengan kunci KMS yang tidak disertakan dalam parameter aturan.

Pengidentifikasi: CLOUDWATCH_LOG_GROUP_ENCRYPTED

Jenis Sumber Daya: AWS::Logs::LogGroup

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Timur Tengah (UEA), Asia Pasifik (Taipei)

Parameter:

KmsKeyId (Opsional), Tipe: String

Amazon Resource Name (ARN) dari ID untuk kunci KMS yang digunakan untuk mengenkripsi grup log.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

cloud-trail-cloud-watch-logs-diaktifkan

Memeriksa apakah AWS CloudTrail jejak dikonfigurasi untuk mengirim log ke CloudWatch log. Jejaknya NON_COMPLIANT jika CloudWatchLogsLogGroupArn properti jejak kosong.

Pengidentifikasi: CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED

Jenis Sumber Daya: AWS::CloudTrail::Trail

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

expectedDeliveryWindowUsia (Opsional), Jenis: int

Usia maksimum dalam jam pengiriman terbaru ke CloudWatch log yang memenuhi kepatuhan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

cloudtrail-diaktifkan

> **Important**
>
> Untuk aturan ini, pengidentifikasi aturan (CLOUD_TRAIL_ENABLED) dan nama aturan (cloudtrail-enabled) berbeda.

Memeriksa apakah AWS CloudTrail jejak diaktifkan di AWS akun Anda. Aturannya adalah NON_COMPLIANT jika jejak tidak diaktifkan. Secara opsional, aturan memeriksa bucket S3 tertentu, topik Amazon Simple Notification Service (Amazon SNS), dan grup log. CloudWatch

Pengidentifikasi: CLOUD_TRAIL_ENABLED

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

s3 BucketName (Opsional), Tipe: String

Nama bucket S3 CloudTrail untuk mengirimkan file log ke.

snsTopicArn (Opsional), Tipe: String

SNS topik ARN CloudTrail untuk digunakan untuk notifikasi.

cloudWatchLogsLogGroupArn (Opsional), Tipe: String

CloudWatch log grup ARN untuk mengirim data CloudTrail ke.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

cloud-trail-encryption-enabled

Memeriksa AWS CloudTrail apakah dikonfigurasi untuk menggunakan enkripsi sisi server (SSE) AWS Key Management Service (AWS KMS) enkripsi. Aturannya adalah COMPLIANT jika KmsKeyId didefinisikan.

Pengidentifikasi: CLOUD_TRAIL_ENCRYPTION_ENABLED

Jenis Sumber Daya: AWS::CloudTrail::Trail

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

cloud-trail-log-file-validasi-diaktifkan

Memeriksa apakah AWS CloudTrail membuat file intisari yang ditandatangani dengan log. AWS merekomendasikan bahwa validasi file harus diaktifkan di semua jalur. Aturannya adalah NON_COMPLIANT jika validasi tidak diaktifkan.

Pengidentifikasi: CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED

Jenis Sumber Daya: AWS::CloudTrail::Trail

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

cmk-backing-key-rotation-diaktifkan

Memeriksa apakah rotasi kunci otomatis diaktifkan untuk setiap kunci dan cocok dengan ID kunci AWS KMS yang dibuat pelanggan. Aturannya adalah NON_COMPLIANT jika peran perekam AWS Config untuk sumber daya tidak memiliki izin. kms: DescribeKey

> **Note**
>
> Rotasi kunci otomatis tidak didukung untuk kunci KMS asimetris, kunci KMS HMAC, kunci KMS dengan bahan kunci impor, atau kunci KMS di toko kunci khusus.

Pengidentifikasi: CMK_BACKING_KEY_ROTATION_ENABLED

Jenis Sumber Daya: AWS::KMS::Key

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Timur Tengah (UEA)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

codebuild-project-artifact-encryption

Memeriksa apakah sebuah AWS CodeBuild proyek telah mengaktifkan enkripsi untuk semua artefaknya. Aturannya adalah NON_COMPLIANT jika 'EncryptionDisabled' disetel ke 'true' untuk konfigurasi artefak primer atau sekunder (jika ada).

Pengidentifikasi: CODEBUILD_PROJECT_ARTIFACT_ENCRYPTION

Jenis Sumber Daya: AWS::CodeBuild::Project

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

codebuild-project-environment-privileged-periksa

Memeriksa apakah lingkungan AWS CodeBuild proyek memiliki mode istimewa yang diaktifkan. Aturannya adalah NON_COMPLIANT untuk CodeBuild proyek jika 'PrivilegedMode' disetel ke 'true'.

Pengidentifikasi: CODEBUILD_PROJECT_ENVIRONMENT_PRIVILEGED_CHECK

Jenis Sumber Daya: AWS::CodeBuild::Project

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Eropa (Zuryol) lich) Wilayah

Parameter:

ExemptedProjects (Opsional), Jenis: CSV

> Daftar nama CodeBuild proyek yang dipisahkan koma yang diizinkan memiliki 'PrivilegedMode' dengan nilai 'benar'.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

codebuild-project-envvar-awscred-periksa

Memeriksa apakah proyek berisi variabel lingkungan _ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY. AWS Aturannya adalah NON_COMPLIANT ketika variabel lingkungan proyek berisi kredenal teks biasa.

Pengidentifikasi: CODEBUILD_PROJECT_ENVVAR_ AWSCRED_CHECK

Jenis Sumber Daya: AWS::CodeBuild::Project

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

codebuild-project-logging-enabled

Memeriksa apakah lingkungan AWS CodeBuild proyek memiliki setidaknya satu opsi log diaktifkan. Aturannya adalah NON_COMPLIANT jika status semua konfigurasi log yang ada disetel ke 'DISABLED'.

Pengidentifikasi: CODEBUILD_PROJECT_LOGGING_ENABLED

Jenis Sumber Daya: AWS::CodeBuild::Project

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

s3 BucketNames (Opsional), Tipe: String

Daftar nama bucket Amazon S3 yang dipisahkan koma yang harus dikirimkan log jika log S3 dikonfigurasi.

cloudWatchGroupNama (Opsional), Tipe: String

Daftar nama grup CloudWatch log Amazon yang dipisahkan koma yang harus dikirimkan log jika CloudWatch log dikonfigurasi.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

codebuild-project-s3-log-terenkripsi

Memeriksa apakah AWS CodeBuild proyek yang dikonfigurasi dengan Amazon S3 Logs mengaktifkan enkripsi untuk lognya. Aturannya adalah NON_COMPLIANT jika 'EncryptionDisabled' disetel ke 'true' dalam S3 proyek. LogsConfig CodeBuild

Pengidentifikasi: CODEBUILD_PROJECT_S3_LOGS_ENCRYPTED

Jenis Sumber Daya: AWS::CodeBuild::Project

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

ExemptedProjects (Opsional), Jenis: CSV

> Daftar nama CodeBuild proyek yang dipisahkan koma yang diizinkan untuk menampilkan log yang tidak terenkripsi.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

codebuild-project-source-repo-url-periksa

Memeriksa apakah URL repositori sumber Bitbucket berisi kredenal masuk atau tidak. Aturannya adalah NON_COMPLIANT jika URL berisi informasi login dan COMPLIANT jika tidak.

Pengidentifikasi: CODEBUILD_PROJECT_SOURCE_REPO_URL_CHECK

Jenis Sumber Daya: AWS::CodeBuild::Project

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

codebuild-report-group-encrypted-saat istirahat

Memeriksa apakah grup AWS CodeBuild laporan memiliki enkripsi saat pengaturan istirahat diaktifkan. Aturannya adalah NON_COMPLIANT jika '' adalah EncryptionDisabled 'benar'.

Pengidentifikasi: CODEBUILD_REPORT_GROUP_ENCRYPTED_AT_REST

Jenis Sumber Daya: AWS::CodeBuild::ReportGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

codedeploy-auto-rollback-monitor-diaktifkan

Memeriksa apakah grup penyebaran dikonfigurasi dengan rollback penerapan otomatis dan pemantauan penerapan dengan alarm terpasang. Aturannya adalah NON_COMPLIANT jika AutoRollbackConfiguration atau AlarmConfiguration belum dikonfigurasi atau tidak diaktifkan.

Pengidentifikasi: CODEPLOY_AUTO_ROLLBACK_MONITOR_ENABLED

Jenis Sumber Daya: AWS::CodeDeploy::DeploymentGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

codedeploy-deployment-group-auto-rollback-diaktifkan

Memeriksa apakah grup AWS CodeDeploy penerapan mengaktifkan konfigurasi rollback otomatis. Aturannya adalah NON_COMPLIANT jika konfigurasi. autoRollbackConfiguration.enabled salah atau tidak ada.

Pengidentifikasi: CODEPLOY_DEPLOYMENT_GROUP_AUTO_ROLLBACK_ENABLED

Jenis Sumber Daya: AWS::CodeDeploy::DeploymentGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

codedeploy-deployment-group-outdated-instances-pembaruan

Memeriksa apakah grup AWS CodeDeploy penerapan secara otomatis memperbarui instance yang sudah ketinggalan zaman. Aturannya adalah NON_COMPLIANT jika konfigurasi. outdatedInstancesStrategy adalah 'ABAIKAN'.

Pengidentifikasi: CODEPLOY_DEPLOYMENT_GROUP_OUTDATED_INSTANCES_UPDATE

Jenis Sumber Daya: AWS::CodeDeploy::DeploymentGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

codedeploy-ec2- minimum-healthy-hosts-configured

Memeriksa apakah grup penerapan untuk EC2 /On-Premise Compute Platform dikonfigurasi dengan persentase armada host sehat minimum atau jumlah host yang lebih besar dari atau sama dengan ambang input. Aturannya adalah NON_COMPLIANT jika keduanya berada di bawah ambang batas.

Pengidentifikasi: EC2 CODEDEPLOY_ _MINIMUM_HEALTHY_HOSTS_CONFIGURATED

Jenis Sumber Daya: AWS::CodeDeploy::DeploymentGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia

Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

minimumHealthyHostsFleetPercent (Opsional), Jenis: int, Default: 66

Persentase minimum armada tuan rumah yang sehat selama penyebaran. Nilai default diatur ke 66 persen.

minimumHealthyHostsHostCount (Opsional), Jenis: int, Default: 1

Jumlah minimum host sehat dalam armada selama penyebaran. Nilai default diatur ke 1.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan

Memeriksa apakah grup penerapan untuk Lambda Compute Platform tidak menggunakan konfigurasi penerapan default. Aturannya adalah NON_COMPLIANT jika grup penerapan menggunakan konfigurasi penerapan '. CodeDeployDefault LambdaAllAtOnce'.

Pengidentifikasi: CODEPLOY_LAMBDA_ALLATONCE_TRAFFIC_SHIFT_DISABLED

Jenis Sumber Daya: AWS::CodeDeploy::DeploymentGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

codeguruprofiler-profiling-group-tagged

Memeriksa apakah grup CodeGuru profil Amazon Profiler memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: CODEGURUPROFILER_PROFILING_GROUP_TAGGED

Jenis Sumber Daya: AWS::CodeGuruProfiler::ProfilingGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Eropa (Stockholm), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Wilayah Asia Pasifik (Sydney)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

codegururreviewer-repository-association-tagged

Memeriksa apakah asosiasi CodeGuru repositori Amazon Reviewer memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: CODEGURUREVIEWER_REPOSITORY_ASSOCIATION_TAGGED

Jenis Sumber Daya: AWS::CodeGuruReviewer::RepositoryAssociation

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Eropa (Stockholm), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Wilayah Asia Pasifik (Sydney)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

codepipeline-deployment-count-check

Memeriksa apakah tahap penerapan pertama AWS CodePipeline melakukan lebih dari satu penerapan. Secara opsional memeriksa apakah setiap tahapan berikutnya yang tersisa disebarkan ke lebih dari jumlah penerapan yang ditentukan (). `deploymentLimit`

Pengidentifikasi: CODEPIPELINE_DEPLOYMENT_COUNT_CHECK

Jenis Sumber Daya: AWS::CodePipeline::Pipeline

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (Bahrain), Tiongkok (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Afrika (Cape Town), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur), AWS GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

DeploymentLimit (Opsional), Jenis: int

> Jumlah maksimum penyebaran yang dapat dilakukan setiap tahap.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

codepipeline-region-fanout-check

Memeriksa apakah setiap tahap dalam AWS CodePipeline penyebaran lebih dari N kali jumlah wilayah yang AWS CodePipeline telah dikerahkan di semua tahap gabungan sebelumnya, di mana N adalah nomor fanout wilayah. Tahap penyebaran pertama dapat diterapkan ke maksimum satu wilayah dan tahap penyebaran kedua dapat diterapkan ke jumlah maksimum yang ditentukan dalam. `regionFanoutFactor` Jika Anda tidak memberikan`regionFanoutFactor`, secara default nilainya adalah tiga. Misalnya: Jika tahap penyebaran pertama diterapkan ke satu wilayah dan tahap penyebaran ke-2 diterapkan ke tiga wilayah, tahap penyebaran ke-3 dapat diterapkan ke 12 wilayah, yaitu jumlah tahapan sebelumnya dikalikan dengan nomor fanout wilayah (tiga). Aturannya adalah NON_COMPLIANT jika penerapan di lebih dari satu wilayah di tahap 1 atau tiga wilayah di tahap ke-2 atau 12 wilayah di tahap ke-3.

Pengidentifikasi: CODEPIPELINE_REGION_FANOUT_CHECK

Jenis Sumber Daya: AWS::CodePipeline::Pipeline

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Asia Pasifik (Mumbai), Eropa (Paris), AS Timur (Ohio), Eropa (Irlandia), Timur Tengah (UEA), Eropa (Frankfurt), Amerika Selatan (Sao Paulo), Asia Pasifik (Hyderabad), AS Timur (Virginia N.), Asia Pasifik (Seoul), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), AS Barat (California N.), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Israel (Tel Aviv), Wilayah Kanada (Tengah)

Parameter:

regionFanoutFactor (Opsional), Jenis: int, Default: 3

> Jumlah wilayah yang AWS CodePipeline telah dikerahkan di semua tahap sebelumnya adalah jumlah wilayah yang dapat diterima dari setiap tahap yang dapat digunakan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

cognito-identity-pool-unauth-akses-cek

Memeriksa apakah Kumpulan Identitas Amazon Cognito mengizinkan identitas yang tidak diautentikasi. Aturannya adalah NON_COMPLIANT jika Identity Pool dikonfigurasi untuk mengizinkan identitas yang tidak diautentikasi.

Pengidentifikasi: COGNITO_IDENTITY_POOL_UNAUTH_ACCESS_CHECK

Jenis Sumber Daya: AWS::Cognito::IdentityPool

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Seoul), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

cognito-user-pool-advanced-keamanan diaktifkan

Memeriksa apakah kumpulan pengguna Amazon Cognito memiliki keamanan lanjutan yang diaktifkan untuk otentikasi standar. Aturannya adalah NON_COMPLIANT jika keamanan lanjutan tidak diaktifkan. Secara opsional, Anda dapat menentukan mode keamanan lanjutan untuk diperiksa aturan.

Pengidentifikasi: COGNITO_USER_POOL_ADVANCED_SECURITY_ENABLED

Jenis Sumber Daya: AWS::Cognito::UserPool

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Afrika (Cape Town), Timur Tengah (UEA), Asia Pasifik (Hong Kong), Asia

Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

SecurityMode (Opsional), Tipe: String

> Nilai string dari mode keamanan lanjutan untuk aturan yang akan diperiksa. Jika disediakan, aturannya adalah NON_COMPLIANT jika mode keamanan lanjutan untuk kumpulan pengguna tidak cocok dengan nilai parameter ini. Nilai yang valid adalah AUDIT dan DITEGAKKAN

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

cognito-user-pool-tagged

Memeriksa apakah kumpulan pengguna Amazon Cognito memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: COGNITO_USER_POOL_TAGGED

Jenis Sumber Daya: AWS::Cognito::UserPool

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

connect-instance-logging-enabled

Memeriksa apakah instans Amazon Connect mengaktifkan log alur di grup CloudWatch log Amazon. Aturannya adalah NON_COMPLIANT jika instance Amazon Connect tidak mengaktifkan flow log.

Pengidentifikasi: CONNECT_INSTANCE_LOGGING_ENABLED

Jenis Sumber Daya: AWS::Connect::Instance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Afrika (Cape Town), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Seoul), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Wilayah Kanada (Tengah)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

customerprofiles-object-type-allow-pembuatan profil

Memeriksa apakah jenis objek Amazon Connect Customer Profiles memungkinkan pembuatan profil standar baru jika tidak ada. Aturannya adalah NON_COMPLIANT jika konfigurasi. AllowProfileCreation adalah palsu.

Pengidentifikasi: CUSTOMERPROFILES_OBJECT_TYPE_ALLOW_PROFILE_CREATION

Jenis Sumber Daya: AWS::CustomerProfiles::ObjectType

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Afrika (Cape Town), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Seoul), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Wilayah Kanada (Tengah)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

customerprofiles-object-type-tagged

Memeriksa apakah jenis objek Amazon Connect Customer Profiles memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: CUSTOMERPROFILES_OBJECT_TYPE_TAGGED

Jenis Sumber Daya: AWS::CustomerProfiles::ObjectType

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Afrika (Cape Town), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Seoul), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Wilayah Kanada (Tengah)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

custom-eventbus-policy-attached

Memeriksa apakah bus acara EventBridge khusus Amazon memiliki kebijakan berbasis sumber daya yang dilampirkan. Aturannya adalah NON_COMPLIANT jika kebijakan bus acara khusus tidak memiliki kebijakan berbasis sumber daya terlampir.

Pengidentifikasi: CUSTOM_EVENTBUS_POLICY_ATTACHED

Jenis Sumber Daya: AWS::Events::EventBus

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), AWS GovCloud (AS-Timur), AWS GovCloud (AS-Barat), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

custom-schema-registry-policy-Terlampir

Memeriksa apakah pendaftar EventBridge skema Amazon khusus memiliki kebijakan sumber daya yang dilampirkan. Aturannya adalah NON_COMPLIANT untuk pendaftar skema kustom tanpa kebijakan sumber daya yang dilampirkan.

Pengidentifikasi: CUSTOM_SCHEMA_REGISTRY_POLICY_ATTACHED

Jenis Sumber Daya: AWS::EventSchemas::Registry

Jenis pemicu: Berkala

Wilayah AWS: Hanya tersedia di Eropa (Stockholm), Asia Pasifik (Mumbai), Eropa (Paris), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), Amerika Selatan (Sao Paulo), Asia Pasifik (Hong Kong), AS Timur (Virginia N.), Asia Pasifik (Seoul), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), AS Barat (California N.), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Wilayah Kanada (Tengah)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

cw-loggroup-retention-period-periksa

Memeriksa apakah periode CloudWatch LogGroup retensi Amazon disetel ke lebih dari 365 hari atau periode retensi tertentu. Aturannya adalah NON_COMPLIANT jika periode retensi kurang dari`MinRetentionTime`, jika ditentukan, atau 365 hari.

> **Note**
>
> Jika pengaturan retensi adalah “Jangan pernah kedaluwarsa” untuk grup log, aturan ditandai sebagai COMPLIANT.

Pengidentifikasi: CW_LOGGROUP_RETENTION_PERIOD_CHECK

Jenis Sumber Daya: AWS::Logs::LogGroup

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Timur Tengah (UEA)

Parameter:

LogGroupNames (Opsional), Jenis: CSV

Daftar nama Grup Log yang dipisahkan koma untuk memeriksa periode retensi.

MinRetentionTime (Opsional), Jenis: int

Tentukan waktu retensi dalam beberapa hari. Nilai yang valid adalah: 1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365, 400, 545, 731, 1827, dan 3653. Periode retensi default adalah 365 hari.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

datasync-task-data-verification-diaktifkan

Memeriksa apakah AWS DataSync tugas mengaktifkan verifikasi data untuk melakukan verifikasi tambahan di akhir transfer Anda. Aturannya adalah NON_COMPLIANT jika Configuration.OPTIONS. VerifyMode adalah 'tidak'.

Pengidentifikasi: DATASYNC_TASK_DATA_VERIFICATION_ENABLED

Jenis Sumber Daya: AWS::DataSync::Task

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

datasync-task-logging-enabled

Memeriksa apakah AWS DataSync tugas mengaktifkan CloudWatch pencatatan Amazon. Aturannya adalah NON_COMPLIANT jika AWS DataSync tugas tidak mengaktifkan CloudWatch pencatatan Amazon atau jika level logging tidak setara dengan level logging yang Anda tentukan.

Pengidentifikasi: DATASYNC_TASK_LOGGING_ENABLED

Jenis Sumber Daya: AWS::DataSync::Task

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

LogLevel (Opsional), Tipe: String

Nilai string untuk tingkat logging. Nilai yang valid meliputi: 'BASIC' dan 'TRANSFER'. Jika tidak ditentukan, nilai defaultnya adalah 'DASAR'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

datasync-task-tagged

Memeriksa apakah AWS DataSync tugas memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk aturan tersebut. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: DATASYNC_TASK_TAGGED

Jenis Sumber Daya: AWS::DataSync::Task

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

dax-encryption-enabled

Memeriksa apakah klaster Amazon DynamoDB Accelerator (DAX) dienkripsi. Aturannya adalah NON_COMPLIANT jika cluster DAX tidak dienkripsi.

Pengidentifikasi: DAX_ENCRYPTION_ENABLED

Jenis Sumber Daya: AWS::DAX::Cluster

Jenis pemicu: Berkala

Wilayah AWS: Hanya tersedia di Eropa (Stockholm), Tiongkok (Beijing), Asia Pasifik (Mumbai), Eropa (Paris), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), Amerika Selatan (Sao Paulo), AS Timur (Virginia N.), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), AS Barat (California N.), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Eropa (Spanyol), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

dax-tls-endpoint-encryption

Memeriksa apakah klaster Amazon DynamoDB Accelerator (DAX) Anda telah disetel ke TLS. ClusterEndpointEncryptionType Aturannya adalah NON_COMPLIANT jika cluster DAX tidak dienkripsi oleh transport layer security (TLS).

Pengidentifikasi: DAX_TLS_ENDPOINT_ENCRYPTION

Jenis Sumber Daya: AWS::DAX::Cluster

Jenis pemicu: Berkala

Wilayah AWS: Hanya tersedia di Asia Pasifik (Mumbai), Eropa (Paris), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), Amerika Selatan (Sao Paulo), AS Timur (Virginia N.), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), AS Barat (California N.), Asia Pasifik (Singapura), Wilayah Asia Pasifik (Sydney)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

db-instance-backup-enabled

Memeriksa apakah instans RDS DB memiliki cadangan yang diaktifkan. Secara opsional, aturan memeriksa periode retensi cadangan dan jendela cadangan.

Pengidentifikasi: DB_INSTANCE_BACKUP_ENABLED

Jenis Sumber Daya: AWS::RDS::DBInstance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

backupRetentionPeriod (Opsional), Jenis: int

Periode retensi untuk cadangan.

backupRetentionMinimum (Opsional), Jenis: int

Periode retensi minimum untuk cadangan.

preferredBackupWindow (Opsional), Tipe: String

Rentang waktu di mana cadangan dibuat.

checkReadReplicas (Opsional), Jenis: boolean

Memeriksa apakah instans RDS DB memiliki cadangan yang diaktifkan untuk replika baca.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

desired-instance-tenancy

Memeriksa EC2 instance untuk nilai 'tenancy'. Juga memeriksa IDs apakah AMI ditentukan untuk diluncurkan dari mereka AMIs atau jika Host IDs diluncurkan pada Host Khusus tersebut. Aturannya adalah COMPLIANT jika instance cocok dengan host dan AMI, jika ditentukan, dalam daftar.

Pengidentifikasi: DESIRED_INSTANCE_TENANCY

Jenis Sumber Daya: AWS::EC2::Instance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

penyewaan, Tipe: String

Penyewaan instans yang diinginkan. Nilai yang valid adalah DEDICATED, HOST dan DEFAULT.

ImageId (Opsional), Jenis: CSV

Aturan mengevaluasi instance yang diluncurkan hanya dari AMIs dengan yang ditentukan. IDs Pisahkan beberapa AMI IDs dengan koma.

HostID (Opsional), Jenis: CSV

Host EC2 Khusus tempat instans dimaksudkan untuk diluncurkan. IDs Pisahkan beberapa Host IDs dengan koma.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

desired-instance-type

Memeriksa apakah EC2 instance Anda dari jenis instans tertentu. Aturannya adalah NON_COMPLIANT jika EC2 instance tidak ditentukan dalam daftar parameter. Untuk daftar jenis EC2 instans yang didukung, lihat Jenis instans di Panduan EC2 Pengguna untuk Instans Linux.

Pengidentifikasi: DESIRED_INSTANCE_TYPE

Jenis Sumber Daya: AWS::EC2::Instance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

instanceType, Jenis: CSV

Daftar tipe EC2 instance yang dipisahkan koma (misalnya, “t2.small, m4.large, i2.xlarge”).

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

dms-auto-minor-version-tingkatkan periksa

Memeriksa apakah instance replikasi AWS Database Migration Service (AWS DMS) mengaktifkan upgrade versi minor otomatis. Aturannya adalah NON_COMPLIANT jika instance replikasi AWS DMS tidak dikonfigurasi dengan upgrade versi minor otomatis.

Pengidentifikasi: DMS_AUTO_MINOR_VERSION_UPGRADE_CHECK

Jenis Sumber Daya: AWS::DMS::ReplicationInstance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur), AWS GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

dms-endpoint-ssl-configured

Memeriksa apakah titik akhir AWS Database Migration Service (AWS DMS) dikonfigurasi dengan koneksi SSL. Aturannya adalah NON_COMPLIANT jika AWS DMS tidak memiliki koneksi SSL yang dikonfigurasi.

Konteks: Koneksi SSL/TLS menyediakan satu lapisan keamanan dengan mengenkripsi data yang bergerak antara klien Anda dan instance DB. Menggunakan sertifikat server memberikan lapisan keamanan tambahan dengan memvalidasi bahwa koneksi sedang dibuat ke instans Amazon RDS DB. Ia melakukannya dengan memeriksa sertifikat server yang diinstal secara otomatis pada semua instance DB yang Anda berikan. Dengan mengaktifkan koneksi SSL AWS DMS, Anda melindungi kerahasiaan data selama migrasi.

Untuk mengonfigurasi koneksi SSL AWS DMS, lihat Menggunakan untuk mengenkripsi sambungan SSL/TLS ke instans atau cluster DB di Panduan Pengguna Layanan Amazon Relational Database Service.

Pengidentifikasi: DMS_ENDPOINT_SSL_CONFIGURATED

Jenis Sumber Daya: AWS::DMS::Endpoint

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur), AWS GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

dms-endpoint-tagged

Memeriksa apakah titik akhir AWS DMS memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: DMS_ENDPOINT_TAGGED

Jenis Sumber Daya: AWS::DMS::Endpoint

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

dms-mongo-db-authentication-diaktifkan

Memeriksa apakah titik akhir AWS Database Migration Service (AWS DMS) untuk penyimpanan MongoDb data diaktifkan untuk otentikasi berbasis kata sandi dan kontrol akses. Aturannya adalah NON_COMPLIANT jika otentikasi berbasis kata sandi dan kontrol akses tidak diaktifkan.

Pengidentifikasi: DMS_MONGO_DB_AUTHENTICATION_ENABLED

Jenis Sumber Daya: AWS::DMS::Endpoint

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

dms-neptune-iam-authorization-diaktifkan

Memeriksa apakah titik akhir AWS Database Migration Service (AWS DMS) untuk database Amazon Neptune dikonfigurasi dengan otorisasi IAM. Aturannya adalah NON_COMPLIANT jika AWS titik akhir DMS di mana Neptunus adalah target telah disetel ke false. IamAuthEnabled

Pengidentifikasi: DMS_NEPTUNE_IAM_AUTHORIZATION_ENABLED

Jenis Sumber Daya: AWS::DMS::Endpoint

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Afrika (Cape Town), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Eropa (Milan), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

dms-redis-tls-enabled

Memeriksa apakah titik akhir AWS Database Migration Service (AWS DMS) untuk penyimpanan data Redis diaktifkan untuk TLS/SSL enkripsi data yang dikomunikasikan dengan titik akhir lainnya. Aturannya adalah NON_COMPLIANT jika TLS/SSL enkripsi tidak diaktifkan.

Pengidentifikasi: DMS_REDIS_TLS_ENABLED

Jenis Sumber Daya: AWS::DMS::Endpoint

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

dms-replication-not-public

Memeriksa apakah instance replikasi AWS Database Migration Service (AWS DMS) bersifat publik. Aturannya adalah NON_COMPLIANT jika PubliclyAccessible bidang disetel ke true.

Pengidentifikasi: DMS_REPLICATION_NOT_PUBLIC

Jenis Sumber Daya: AWS::DMS::ReplicationInstance

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

dms-replication-task-sourcedb-logging

Memeriksa apakah logging diaktifkan dengan tingkat keparahan yang valid untuk tugas replikasi AWS DMS dari database sumber. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan atau log untuk tugas replikasi DMS dari database sumber memiliki tingkat keparahan yang tidak valid.

Pengidentifikasi: DMS_REPLICATION_TASK_SOURCEDB_LOGGING

Jenis Sumber Daya: AWS::DMS::ReplicationTask

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur), AWS GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

dms-replication-task-tagged

Memeriksa apakah tugas replikasi AWS DMS memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: DMS_REPLICATION_TASK_TAGGED

Jenis Sumber Daya: AWS::DMS::ReplicationTask

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

dms-replication-task-targetdb-logging

Memeriksa apakah logging diaktifkan dengan tingkat keparahan yang valid untuk peristiwa tugas replikasi AWS DMS dari database target. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan atau pencatatan tugas replikasi dari database target memiliki tingkat keparahan yang tidak valid.

Pengidentifikasi: DMS_REPLICATION_TASK_TARGETDB_LOGGING

Jenis Sumber Daya: AWS::DMS::ReplicationTask

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur), AWS GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

docdb-cluster-audit-logging-diaktifkan

Memeriksa apakah klaster CloudWatch instans Amazon DocumentDB (dengan kompatibilitas MongoDB) mengaktifkan ekspor log untuk log audit. Aturannya adalah NON_COMPLIANT jika klaster instans Amazon DocumentDB tidak mengaktifkan ekspor log untuk log audit. CloudWatch

Pengidentifikasi: DOCDB_CLUSTER_AUDIT_LOGGING_ENABLED

Jenis Sumber Daya: AWS::RDS::DBCluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Eropa (Stockholm), Timur Tengah (Bahrain), Tiongkok (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Afrika (Cape Town), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), AS Barat (California N.), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

docdb-cluster-backup-retention-periksa

Memeriksa apakah periode retensi klaster Amazon Document DB disetel ke jumlah hari tertentu. Aturannya adalah NON_COMPLIANT jika periode retensi kurang dari nilai yang ditentukan oleh parameter.

Pengidentifikasi: DOCDB_CLUSTER_BACKUP_RETENTION_CHECK

Jenis Sumber Daya: AWS::RDS::DBCluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Eropa (Stockholm), Timur Tengah (Bahrain), Tiongkok (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Afrika (Cape Town), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), AS Barat (California N.), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

minimumBackupRetentionPeriode (Opsional), Jenis: int

> Backup hari minimum harus disimpan. Nilai valid 1 hingga 35, nilai default adalah 7. Aturan ini adalah NON_COMPLIANT jika nilainya lebih besar dari ". backupRetentionPeriod

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

docdb-cluster-deletion-protection-diaktifkan

Memeriksa apakah klaster Amazon DocumentDB (dengan kompatibilitas MongoDB) mengaktifkan perlindungan penghapusan. Aturannya adalah NON_COMPLIANT jika klaster Amazon DocumentDB memiliki bidang DeletionProtection disetel ke false.

Pengidentifikasi: DOCDB_CLUSTER_DELETION_PROTECTION_ENABLED

Jenis Sumber Daya: AWS::RDS::DBCluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Eropa (Stockholm), Timur Tengah (Bahrain), Tiongkok (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Afrika (Cape Town), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), AS Barat (California N.), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

docdb-cluster-encrypted

Memeriksa apakah enkripsi penyimpanan diaktifkan untuk klaster Amazon DocumentDB Anda (dengan kompatibilitas MongoDB). Aturannya adalah NON_COMPLIANT jika enkripsi penyimpanan tidak diaktifkan.

Pengidentifikasi: DOCDB_CLUSTER_ENCRYPTED

Jenis Sumber Daya: AWS::RDS::DBCluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Eropa (Stockholm), Timur Tengah (Bahrain), Tiongkok (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Afrika (Cape Town), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), AS Barat (California N.), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

kmsKeyArns (Opsional), Jenis: CSV

> Daftar kunci KMS yang dipisahkan koma ARNs untuk dibandingkan dengan KmsKey ID cluster terenkripsi.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

docdb-cluster-encrypted-in-transit

Memeriksa apakah koneksi ke cluster Amazon DocumentDB dikonfigurasi untuk menggunakan enkripsi dalam perjalanan. Aturannya adalah NON_COMPLIANT jika grup parameter tidak “sinkron”, atau parameter TLS disetel ke “dinonaktifkan” atau nilai dalam. `excludeTlsParameters`

Pengidentifikasi: DOCDB_CLUSTER_ENCRYPTED_IN_TRANSIT

Jenis Sumber Daya: AWS::RDS::DBCluster

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Eropa (Stockholm), Timur Tengah (Bahrain), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Afrika (Cape Town), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), AS Barat (California N.), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calon Gary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

excludeTlsParameters (Opsional), Jenis: CSV

> Daftar parameter cluster TLS yang dipisahkan koma agar aturan TIDAK diperiksa. Nilai default: 'dinonaktifkan'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

docdb-cluster-snapshot-public-dilarang

Memeriksa apakah snapshot cluster manual Amazon DocumentDB bersifat publik. Aturannya adalah NON_COMPLIANT jika ada snapshot cluster manual Amazon DocumentDB yang bersifat publik.

Pengidentifikasi: DOCDB_CLUSTER_SNAPSHOT_PUBLIC_FORBIDNED

Jenis Sumber Daya: AWS::RDS::DBClusterSnapshot

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Asia Pasifik (Mumbai), Eropa (Paris), AS Timur (Ohio), Eropa (Irlandia), Timur Tengah (UEA), Eropa (Frankfurt), Amerika Selatan (Sao Paulo), Asia Pasifik (Hong Kong), Asia Pasifik (Hyderabad), AS Timur (Virginia N), Asia Pasifik (Seoul), Eropa (London), Eropa (Milan), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Wilayah Kanada (Tengah)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

dynamodb-autoscaling-enabled

Memeriksa apakah tabel Amazon DynamoDB atau indeks sekunder global dapat read/write memproses kapasitas menggunakan mode sesuai permintaan atau mode yang disediakan dengan penskalaan otomatis diaktifkan. Aturannya adalah NON_COMPLIANT jika salah satu mode digunakan tanpa penskalaan otomatis diaktifkan

Pengidentifikasi: DYNAMODB_AUTOSCALING_ENABLED

Jenis Sumber Daya: AWS::DynamoDB::Table

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

minProvisionedReadKapasitas (Opsional), Jenis: int

Jumlah minimum unit yang harus disediakan dengan kapasitas baca di grup Auto Scaling.

maxProvisionedReadKapasitas (Opsional), Jenis: int

Jumlah maksimum unit yang harus disediakan dengan kapasitas baca di grup Auto Scaling.

targetReadUtilization (Opsional), Jenis: ganda

Target persentase pemanfaatan untuk kapasitas baca. Pemanfaatan target dinyatakan dalam rasio kapasitas konsumsi terhadap kapasitas yang disediakan.

minProvisionedWriteKapasitas (Opsional), Jenis: int

Jumlah minimum unit yang harus disediakan dengan kapasitas tulis dalam grup Auto Scaling.

maxProvisionedWriteKapasitas (Opsional), Jenis: int

Jumlah maksimum unit yang harus disediakan dengan kapasitas tulis dalam grup Auto Scaling.

targetWriteUtilization (Opsional), Jenis: ganda

Persentase pemanfaatan target untuk kapasitas tulis. Pemanfaatan target dinyatakan dalam rasio kapasitas konsumsi terhadap kapasitas yang disediakan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

dynamodb-in-backup-plan

Memeriksa apakah tabel Amazon DynamoDB ada di AWS Paket Cadangan. Aturannya adalah NON_COMPLIANT jika tabel Amazon DynamoDB tidak ada dalam paket Backup apa pun. AWS

Pengidentifikasi: DYNAMODB_IN_BACKUP_PLAN

Jenis Sumber Daya: AWS::DynamoDB::Table

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

dynamodb-last-backup-recovery-point-dibuat

Memeriksa apakah titik pemulihan dibuat untuk Tabel Amazon DynamoDB dalam periode yang ditentukan. Aturannya adalah NON_COMPLIANT jika Tabel DynamoDB tidak memiliki titik pemulihan yang sesuai yang dibuat dalam periode waktu yang ditentukan.

Pengidentifikasi: DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED

Jenis Sumber Daya: AWS::DynamoDB::Table

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

ResourceTags (Opsional), Tipe: String

Tag Tabel DynamoDB untuk aturan untuk memeriksa, dalam format JSON. `{"tagkey" : "tagValue"}`

ResourceID (Opsional), Tipe: String

Nama DynamoDB Tabel untuk aturan yang akan diperiksa.

recoveryPointAgeNilai (Opsional), Jenis: int, Default: 1

Nilai numerik untuk usia maksimum yang diizinkan. Tidak lebih dari 744 jam, 31 untuk hari.

recoveryPointAgeUnit (Opsional), Tipe: String, Default: hari

Satuan waktu untuk usia maksimum yang diizinkan. Nilai yang diterima: 'jam', 'hari'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

dynamodb-meets-restore-time-target

Memeriksa apakah waktu pemulihan Tabel Amazon DynamoDB memenuhi durasi yang ditentukan. Aturannya adalah NON_COMPLIANT jika LatestRestoreExecutionTimeMinutes dari DynamoDB Table lebih besar dari menit. maxRestoreTime

Pengidentifikasi: DYNAMODB_MEETS_RESTORE_TIME_TARGET

Jenis Sumber Daya: AWS::DynamoDB::Table

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

maxRestoreTime, Jenis: int

Nilai numerik untuk runtime pemulihan maksimum yang diizinkan.

ResourceTags (Opsional), Tipe: String

Tag Tabel DynamoDB untuk aturan untuk memeriksa, dalam format JSON.

ResourceID (Opsional), Tipe: String

Nama DynamoDB Tabel untuk aturan yang akan diperiksa.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

dynamodb-pitr-enabled

Memeriksa apakah point-in-time pemulihan (PITR) diaktifkan untuk tabel Amazon DynamoDB. Aturannya adalah NON_COMPLIANT jika PITR tidak diaktifkan untuk tabel DynamoDB.

Pengidentifikasi: DYNAMODB_PITR_ENABLED

Jenis Sumber Daya: AWS::DynamoDB::Table

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

dynamodb-resources-protected-by-rencana cadangan

Memeriksa apakah tabel Amazon DynamoDB dilindungi oleh paket cadangan. Aturannya adalah NON_COMPLIANT jika Tabel DynamoDB tidak dicakup oleh rencana cadangan.

Pengidentifikasi: DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Jenis Sumber Daya: AWS::DynamoDB::Table

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

ResourceTags (Opsional), Tipe: String

Tag untuk tabel DynamoDB untuk aturan untuk memeriksa, dalam format JSON. `{"tagkey" : "tagValue"}`

ResourceID (Opsional), Tipe: String

Nama tabel DynamoDB untuk aturan yang akan diperiksa.

crossRegionList (Opsional), Tipe: String

Daftar wilayah tujuan yang dipisahkan koma untuk salinan cadangan lintas wilayah yang akan disimpan

crossAccountList (Opsional), Tipe: String

Daftar akun tujuan yang dipisahkan koma untuk salinan cadangan lintas akun yang akan disimpan

maxRetentionDays (Opsional), Jenis: int

Periode retensi maksimum dalam beberapa hari untuk Backup Vault Lock

minRetentionDays (Opsional), Jenis: int

Periode retensi minimum dalam beberapa hari untuk Backup Vault Lock

backupVaultLockPeriksa (Opsional), Tipe: String

Nilai yang diterima: 'Benar' atau 'False'. Masukkan 'Benar' untuk aturan untuk memeriksa apakah sumber daya dicadangkan di brankas yang terkunci

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

dynamodb-table-deletion-protection-diaktifkan

Memeriksa apakah tabel Amazon DynamoDB memiliki perlindungan penghapusan yang disetel ke diaktifkan. Aturannya adalah NON_COMPLIANT jika tabel memiliki proteksi penghapusan yang disetel ke dinonaktifkan.

Pengidentifikasi: DYNAMODB_TABLE_DELETION_PROTECTION_ENABLED

Jenis Sumber Daya: AWS::DynamoDB::Table

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

dynamodb-table-encrypted-kms

Memeriksa apakah tabel Amazon DynamoDB dienkripsi AWS dengan Key Management Service (KMS). Aturannya adalah NON_COMPLIANT jika tabel Amazon DynamoDB tidak dienkripsi dengan KMS. AWS Aturannya juga NON_COMPLIANT jika kunci AWS KMS terenkripsi tidak ada dalam parameter input. `kmsKeyArns`

Pengidentifikasi: DYNAMODB_TABLE_ENCRYPTED_KMS

Jenis Sumber Daya: AWS::DynamoDB::Table

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei)

Parameter:

kmsKeyArns (Opsional), Jenis: CSV

Daftar kunci AWS KMS yang dipisahkan koma ARNs diizinkan untuk mengenkripsi Tabel Amazon DynamoDB.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

dynamodb-table-encryption-enabled

Memeriksa apakah tabel Amazon DynamoDB dienkripsi dan memeriksa statusnya. Aturannya adalah COMPLIANT jika status diaktifkan atau diaktifkan.

Pengidentifikasi: DYNAMODB_TABLE_ENCRYPTION_ENABLED

Jenis Sumber Daya: AWS::DynamoDB::Table

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Eropa (Stockholm), Timur Tengah (Bahrain), Asia Pasifik (Jakarta), Afrika (Cape Town), Asia Pasifik (Hong Kong), Asia Pasifik (Hyderabad), Asia Pasifik (Osaka), Eropa (Milan), Eropa (Spanyol), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

dynamodb-throughput-limit-check

Memeriksa apakah throughput DynamoDB yang disediakan mendekati batas maksimum untuk akun Anda. Secara default, aturan memeriksa apakah throughput yang disediakan melebihi ambang batas 80 persen dari batas akun Anda.

Pengidentifikasi: DYNAMODB_THROUGHPUT_LIMIT_CHECK

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei)

Parameter:

RCUThresholdPersentase akun (Opsional), Jenis: int, Default: 80

Persentase unit kapasitas baca yang disediakan untuk akun Anda. Ketika nilai ini tercapai, aturan ditandai sebagai tidak patuh.

WCUThresholdPersentase akun (Opsional), Jenis: int, Default: 80

Persentase unit kapasitas tulis yang disediakan untuk akun Anda. Ketika nilai ini tercapai, aturan ditandai sebagai tidak patuh.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ebs-in-backup-plan

Periksa apakah volume Amazon Elastic Block Store (Amazon EBS) ditambahkan dalam paket cadangan Backup. AWS Aturannya adalah NON_COMPLIANT jika volume Amazon EBS tidak disertakan dalam paket cadangan.

Pengidentifikasi: EBS_IN_BACKUP_PLAN

Jenis Sumber Daya: AWS::EC2::Volume

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Melbourne), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ebs-last-backup-recovery-point-dibuat

Memeriksa apakah titik pemulihan dibuat untuk Amazon Elastic Block Store (Amazon EBS). Aturannya adalah NON_COMPLIANT jika volume Amazon EBS tidak memiliki titik pemulihan yang sesuai yang dibuat dalam periode waktu yang ditentukan.

Pengidentifikasi: EBS_LAST_BACKUP_RECOVERY_POINT_CREATED

Jenis Sumber Daya: AWS::EC2::Volume

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

ResourceTags (Opsional), Tipe: String

Tag volume Amazon EBS untuk aturan yang akan diperiksa, dalam format JSON. `{"tagkey" : "tagValue"}`

ResourceID (Opsional), Tipe: String

ID volume Amazon EBS untuk aturan yang akan diperiksa.

recoveryPointAgeNilai (Opsional), Jenis: int, Default: 1

Nilai numerik untuk usia maksimum yang diizinkan. Tidak lebih dari 744 jam, 31 untuk hari.

recoveryPointAgeUnit (Opsional), Tipe: String, Default: hari

Satuan waktu untuk usia maksimum yang diizinkan. Nilai yang diterima: 'jam', 'hari'.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ebs-meets-restore-time-target

Memeriksa apakah waktu pemulihan volume Amazon Elastic Block Store (Amazon EBS) memenuhi durasi yang ditentukan. Aturannya adalah NON_COMPLIANT jika LatestRestoreExecutionTimeMinutes volume Amazon EBS lebih besar dari menit. maxRestoreTime

Pengidentifikasi: EBS_MEETS_RESTORE_TIME_TARGET

Jenis Sumber Daya: AWS::EC2::Volume

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

maxRestoreTime, Jenis: int

Nilai numerik untuk runtime pemulihan maksimum yang diizinkan.

ResourceTags (Opsional), Tipe: String

Tag untuk volume Amazon EBS untuk aturan yang akan diperiksa, dalam format JSON.

ResourceID (Opsional), Tipe: String

ID volume Amazon EBS untuk aturan yang akan diperiksa.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ebs-optimized-instance

Memeriksa apakah pengoptimalan Amazon EBS diaktifkan untuk instans Amazon Elastic Compute Cloud EC2 (Amazon) yang dapat dioptimalkan untuk Amazon EBS. Aturannya adalah NON_COMPLIANT jika pengoptimalan EBS tidak diaktifkan untuk EC2 instans Amazon yang dapat dioptimalkan EBS.

> **Note**
>
> EC2 instance yang dioptimalkan EBS secara default selalu menghasilkan evaluasi aturan kembali. `COMPLIANT`

Pengidentifikasi: EBS_OPTIMIZED_INSTANCE

Jenis Sumber Daya: AWS::EC2::Instance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ebs-resources-in-logically-air-gapped-vault

Memeriksa apakah volume Amazon Elastic Block Store (Amazon EBS) berada dalam lemari besi yang memiliki gap udara secara logis. Aturannya adalah NON_COMPLIANT jika volume Amazon EBS tidak berada dalam brankas dengan gapped udara secara logis dalam periode waktu yang ditentukan.

Pengidentifikasi: EBS_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

Jenis Sumber Daya: AWS::EC2::Volume

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

ResourceTags (Opsional), Tipe: String

Tag volume Amazon EBS untuk aturan yang akan diperiksa, dalam format JSON.

ResourceID (Opsional), Tipe: String

ID volume Amazon EBS untuk aturan yang akan diperiksa.

recoveryPointAgeNilai (Opsional), Jenis: int, Default: 1

Nilai numerik untuk usia maksimum yang diizinkan. Tidak lebih dari 2184 jam, 91 untuk hari.

recoveryPointAgeUnit (Opsional), Tipe: String, Default: hari

Satuan waktu untuk usia maksimum yang diizinkan. Nilai yang diterima: 'jam', 'hari'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ebs-resources-protected-by-rencana cadangan

Memeriksa apakah volume Amazon Elastic Block Store (Amazon EBS) dilindungi oleh paket cadangan. Aturannya adalah NON_COMPLIANT jika volume Amazon EBS tidak dicakup oleh paket cadangan.

Pengidentifikasi: EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Jenis Sumber Daya: AWS::EC2::Volume

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

ResourceTags (Opsional), Tipe: String

Tag untuk volume Amazon EBS untuk aturan yang akan diperiksa, dalam format JSON.
`{"tagkey" : "tagValue"}`

ResourceID (Opsional), Tipe: String

ID volume Amazon EBS untuk aturan yang akan diperiksa.

crossRegionList (Opsional), Tipe: String

Daftar wilayah tujuan yang dipisahkan koma untuk salinan cadangan lintas wilayah yang akan disimpan

crossAccountList (Opsional), Tipe: String

Daftar akun tujuan yang dipisahkan koma untuk salinan cadangan lintas akun yang akan disimpan

maxRetentionDays (Opsional), Jenis: int

Periode retensi maksimum dalam beberapa hari untuk Backup Vault Lock

minRetentionDays (Opsional), Jenis: int

Periode retensi minimum dalam beberapa hari untuk Backup Vault Lock

backupVaultLockPeriksa (Opsional), Tipe: String

Nilai yang diterima: 'Benar' atau 'False'. Masukkan 'Benar' untuk aturan untuk memeriksa apakah sumber daya dicadangkan di brankas yang terkunci

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ebs-snapshot-public-restorable-periksa

Memeriksa apakah snapshot Amazon Elastic Block Store (Amazon EBS) tidak dapat dipulihkan secara publik. Aturannya adalah NON_COMPLIANT jika satu atau beberapa snapshot dengan RestorableByUserIds bidang disetel ke semua, yaitu snapshot Amazon EBS bersifat publik.

Pengidentifikasi: EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Eropa (Spanyol)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ec2- capacity-reservation-tagged

Memeriksa apakah reservasi EC2 kapasitas Amazon memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk aturan tersebut. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: EC2 _CAPACITY_RESERVATION_TAGGED

Jenis Sumber Daya: AWS::EC2::CapacityReservation

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ec2- carrier-gateway-tagged

Memeriksa apakah gateway EC2 operator Amazon memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk aturan tersebut. Aturannya adalah NON_COMPLIANT jika tidak ada tag

atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: EC2 _CARRIER_GATEWAY_TAGGED

Jenis Sumber Daya: AWS::EC2::CarrierGateway

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Eropa (Paris), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Seoul), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Sydney), Wilayah Kanada (Tengah)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ec2- diaktifkan client-vpn-connection-log

Memeriksa apakah titik akhir AWS Client VPN mengaktifkan pencatatan koneksi klien. Aturannya adalah NON_COMPLIANT jika 'Konfigurasi. ConnectionLogOptions.Enabled' disetel ke false.

Pengidentifikasi: _CLIENT_VPN_CONNECTION_LOG_ENABLED EC2

Jenis Sumber Daya: AWS::EC2::ClientVpnEndpoint

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ec2- client-vpn-endpoint-tagged

Memeriksa apakah titik akhir VPN EC2 klien Amazon memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk aturan tersebut. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: EC2 _CLIENT_VPN_ENDPOINT_TAGGED

Jenis Sumber Daya: AWS::EC2::ClientVpnEndpoint

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Tiongkok (Ningxia)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ec2- -semua client-vpn-not-authorize

Memeriksa apakah aturan otorisasi AWS Client VPN mengotorisasi akses koneksi untuk semua klien. Aturannya adalah NON_COMPLIANT jika 'AccessAll' hadir dan disetel ke true.

Pengidentifikasi: EC2 _CLIENT_VPN_NOT_AUTHORIZE_ALL

Jenis Sumber Daya: AWS::EC2::ClientVpnEndpoint

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ec2- dhcp-options-tagged

Memeriksa apakah opsi Amazon EC2 DHCP memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk aturan tersebut. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: EC2 _DHCP_OPTIONS_TAGGED

Jenis Sumber Daya: AWS::EC2::DHCPOptions

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ec2- ebs-encryption-by-default

Memeriksa apakah enkripsi Amazon Elastic Block Store (EBS) diaktifkan secara default. Aturannya adalah NON_COMPLIANT jika enkripsi tidak diaktifkan.

Pengidentifikasi: EC2 _EBS_ENCRYPTION_BY_DEFAULT

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ec2- diaktifkan enis-source-destination-check

Memeriksa apakah EC2 ENIs dikelola oleh pengguna telah mengaktifkan source/destination pemeriksaan. Aturannya adalah NON_COMPLIANT jika source/destination pemeriksaan dinonaktifkan ENIs untuk 'lambda', 'aws_codestar_connections_managed', 'branch', 'efa', 'interface', dan 'quicksight'.

Pengidentifikasi: _ENIS_SOURCE_DESTINATION_CHECK_ENABLED EC2

Jenis Sumber Daya: AWS::EC2::NetworkInterface

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Seoul), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ec2-fleet-tag

Memeriksa apakah EC2 armada Amazon memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: EC2 _FLEET_TAGGED

Jenis Sumber Daya: AWS::EC2::EC 2Armada

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ec2-imdsv2-periksa

Memeriksa apakah versi metadata instans Amazon Elastic Compute Cloud (Amazon EC2) Anda dikonfigurasi dengan Instance Metadata Service Version 2 (). IMDSv2 Aturannya adalah NON_COMPLIANT jika HttpTokens diatur ke opsional.

Pengidentifikasi: EC2 _ IMDSV2 _PERIKSA

Jenis Sumber Daya: AWS::EC2::Instance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ec2- instance-detailed-monitoring-enabled

Memeriksa apakah pemantauan terperinci diaktifkan untuk EC2 instance. Aturannya adalah NON_COMPLIANT jika pemantauan terperinci tidak diaktifkan.

Pengidentifikasi: _INSTANCE_DETAILED_MONITORING_ENABLED EC2

Jenis Sumber Daya: AWS::EC2::Instance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ec2- -ami instance-launched-with-allowed

Memeriksa apakah EC2 instans yang sedang berjalan atau dihentikan diluncurkan dengan Amazon Machine Images (AMIs) yang memenuhi AMIs kriteria Diizinkan. Aturannya adalah NON_COMPLIANT jika AMI tidak memenuhi AMIs kriteria Diizinkan dan AMIs pengaturan yang Diizinkan tidak dinonaktifkan.

Pengidentifikasi: _INSTANCE_LAUNCHED_WITH_ALLOWED_AMI EC2

Jenis Sumber Daya: AWS::EC2::Instance

Jenis pemicu: Perubahan konfigurasi dan Periodik

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

InstanceStateNameList (Opsional), Jenis: CSV

> Daftar status EC2 instans Amazon yang terpisah koma untuk diperiksa aturan. Nilai yang valid adalah “berjalan” dan “berhenti”.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ec2- -manajer instance-managed-by-systems

> **Important**
>
> Untuk aturan ini, pengidentifikasi aturan (EC2_INSTANCE_MANAGED_BY_SSM) dan nama aturan (ec2- -manager) berbeda. instance-managed-by-systems

Memeriksa apakah EC2 instans Amazon Anda dikelola oleh AWS Systems Manager Agen (Agen SSM). Aturannya adalah NON_COMPLIANT jika sebuah EC2 instance berjalan dan Agen SSM dihentikan, atau jika EC2 instance sedang berjalan dan Agen SSM dihentikan.

> **Note**
>
> Aturan tidak akan mengembalikan NON_COMPLIANT jika EC2 instance dihentikan dan Agen SSM sedang berjalan.

Pengidentifikasi: EC2 _INSTANCE_MANAGED_BY_SSM

Jenis Sumber Daya: AWS::EC2::Instance, AWS::SSM::ManagedInstanceInventory

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Timur Tengah (UEA), Asia Pasifik (Taipei)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ec2- instance-multiple-eni-check

Memeriksa apakah Amazon Elastic Compute Cloud (Amazon EC2) menggunakan beberapa Antarmuka Jaringan Elastis (ENIs) atau Adaptor Kain Elastis (EFAs). Aturannya adalah NON_COMPLIANT, EC2 instans Amazon menggunakan beberapa antarmuka jaringan.

Pengidentifikasi: EC2 _INSTANCE_MULTIPLE_ENI_CHECK

Jenis Sumber Daya: AWS::EC2::Instance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

NetworkInterfaceIds (Opsional), Jenis: CSV

Daftar instance jaringan yang dipisahkan koma IDs

Evaluasi Proaktif

Untuk langkah-langkah tentang cara menjalankan aturan ini dalam mode proaktif, lihat Mengevaluasi Sumber Daya Anda dengan AWS Config Aturan. Agar aturan ini mengembalikan COMPLIANT dalam mode proaktif, skema konfigurasi sumber daya untuk StartResourceEvaluationAPI harus menyertakan input berikut, yang dikodekan sebagai string:

```
"ResourceConfiguration":
...
{
   "NetworkInterfaces": "[NetworkInterfaceId-1, NetworkInterfaceId-2,
 NetworkInterfaceId-3, ...]"
}
...
```

Untuk informasi lebih lanjut tentang evaluasi proaktif, lihat Mode Evaluasi.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ec2- instance-no-public-ip

Memeriksa apakah EC2 instance memiliki asosiasi IP publik. Aturannya adalah NON_COMPLIANT jika bidang PublicIP ada di item konfigurasi instance. EC2 Aturan hanya berlaku untuk IPv4.

Konteks: Alamat IP publik dapat membuat EC2 instance dapat diakses langsung dari internet, yang mungkin tidak selalu diinginkan dari sudut pandang keamanan atau kepatuhan:

- Keamanan: Dalam banyak kasus, Anda mungkin tidak ingin EC2 instans Anda memiliki alamat IP publik kecuali mereka harus dapat diakses publik. Memiliki alamat IP publik dapat mengekspos EC2 instans Anda terhadap potensi risiko keamanan, seperti akses atau serangan yang tidak sah.
- Kepatuhan: Berbagai standar kepatuhan seperti PCI, DSS, atau HIPAA memiliki persyaratan khusus mengenai segmentasi jaringan dan kontrol akses. Memastikan bahwa EC2 instans tidak memiliki alamat IP publik yang tidak perlu dapat membantu memastikan kepatuhan terhadap persyaratan ini.

- Manajemen Biaya: Alamat IP publik dapat menimbulkan biaya tambahan, terutama jika ada EC2 contoh yang terus dikaitkan dengannya. Dengan mengidentifikasi EC2 contoh dengan publik IPs yang tidak membutuhkannya, Anda berpotensi mengurangi biaya.

Pengidentifikasi: _INSTANCE_NO_PUBLIC_IP EC2

Jenis Sumber Daya: AWS::EC2::Instance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ec2- instance-profile-attached

Memeriksa apakah sebuah EC2 instans memiliki profil AWS Identity and Access Management (IAM) yang dilampirkan padanya. Aturannya adalah NON_COMPLIANT jika tidak ada profil IAM yang dilampirkan ke instance. EC2

Pengidentifikasi: _INSTANCE_PROFILE_ATTACTED EC2

Jenis Sumber Daya: AWS::EC2::Instance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei), Kanada Barat (Calgary)

Parameter:

IamInstanceProfileArnList (Opsional), Jenis: CSV

> Daftar profil IAM yang dipisahkan koma Nama Sumber Daya Amazon (ARNs) yang dapat dilampirkan ke instans Amazon. EC2

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ec2- -dibuat last-backup-recovery-point

Memeriksa apakah titik pemulihan dibuat untuk instans Amazon Elastic Compute Cloud (Amazon EC2). Aturannya adalah NON_COMPLIANT EC2 jika instance Amazon tidak memiliki titik pemulihan terkait yang dibuat dalam periode waktu yang ditentukan.

Pengidentifikasi: _LAST_BACKUP_RECOVERY_POINT_CREATED EC2

Jenis Sumber Daya: AWS::EC2::Instance

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

ResourceTags (Opsional), Tipe: String

Tag EC2 instans Amazon untuk aturan yang akan diperiksa, dalam format JSON. `{"tagkey" : "tagValue"}`

ResourceID (Opsional), Tipe: String

ID EC2 instans Amazon untuk aturan yang akan diperiksa.

recoveryPointAgeNilai (Opsional), Jenis: int, Default: 1

Nilai numerik untuk usia maksimum yang diizinkan. Tidak lebih dari 744 jam, 31 untuk hari.

recoveryPointAgeUnit (Opsional), Tipe: String, Default: hari

Satuan waktu untuk usia maksimum yang diizinkan. Nilai yang diterima: 'jam', 'hari'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ec2- 2-periksa launch-template-imdsv

Memeriksa apakah versi default Template EC2 Peluncuran Amazon yang saat ini disetel memerlukan instans baru yang diluncurkan untuk menggunakan V2 dari Amazon EC2 Instance Metadata Service (). IMDSv2 Aturannya adalah NON_COMPLIANT jika 'versi Metadata' tidak ditentukan sebagai V2 (). IMDSv2

Pengidentifikasi: EC2 _LAUNCH_TEMPLATE_ IMDSV2 _PERIKSA

Jenis Sumber Daya: AWS::EC2::LaunchTemplate

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur), AWS GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Eropa (Zurich) Wilayah

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ec2- launch-template-public-ip -dinonaktifkan

Memeriksa apakah Templat EC2 Peluncuran Amazon disetel untuk menetapkan alamat IP publik ke Antarmuka Jaringan. Aturannya adalah NON_COMPLIANT jika versi default Template EC2 Peluncuran memiliki setidaknya 1 Antarmuka Jaringan dengan '' disetel ke AssociatePublicIpAddress 'benar'.

Pengidentifikasi: _LAUNCH_TEMPLATE_PUBLIC_IP_DISABLED EC2

Jenis Sumber Daya: AWS::EC2::LaunchTemplate

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur), AWS

GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Eropa (Zurich) Wilayah

Parameter:

exemptedLaunchTemplates (Opsional), Jenis: CSV

> Daftar Template EC2 Peluncuran yang dikecualikan yang dipisahkan koma IDs yang diizinkan memiliki Antarmuka Jaringan dengan AssociatePublicIpAddress nilai yang disetel ke 'benar'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ec2- launch-template-tagged

Memeriksa apakah templat EC2 peluncuran Amazon memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk aturan tersebut. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: EC2 _LAUNCH_TEMPLATE_TAGGED

Jenis Sumber Daya: AWS::EC2::LaunchTemplate

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ec2- managedinstance-applications-blacklisted

Memeriksa apakah tidak ada aplikasi yang ditentukan diinstal pada instance. Secara opsional, tentukan versinya. Versi yang lebih baru tidak akan dicantumkan. Secara opsional, tentukan platform untuk menerapkan aturan hanya untuk instance yang menjalankan platform itu.

Pengidentifikasi: EC2 _MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED

Jenis Sumber Daya: AWS::SSM::ManagedInstanceInventory

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei), Kanada Barat (Calgary)

Parameter:

applicationNames, Jenis: CSV

Daftar nama aplikasi yang dipisahkan koma. Secara opsional, tentukan versi yang ditambahkan dengan ':' (misalnya, 'Chrome:0.5.3, Firefox').

> **Note**
>
> Nama aplikasi harus sama persis. Misalnya, gunakan **`firefox`** di Linux atau **`firefox-compat`** di Amazon Linux. Selain itu, saat ini AWS Config tidak mendukung wildcard untuk parameter ApplicationNames (misalnya,). **`firefox*`**

PlatformType (Opsional), Tipe: String

Jenis platform (misalnya, 'Linux' atau 'Windows').

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ec2- managedinstance-applications-required

Memeriksa apakah semua aplikasi yang ditentukan diinstal pada instance. Secara opsional, tentukan versi minimum yang dapat diterima. Anda juga dapat menentukan platform untuk menerapkan aturan hanya untuk instance yang menjalankan platform itu.

> **Note**
>
> Pastikan agen SSM berjalan pada EC2 instance dan asosiasi untuk mengumpulkan inventaris perangkat lunak aplikasi dibuat. Aturan kembali `NOT_APPLICABLE` jika agen SSM tidak diinstal atau asosiasi belum dibuat atau berjalan.

Pengidentifikasi: EC2 _MANAGEDINSTANCE_APPLICATIONS_REQUIRED

Jenis Sumber Daya: AWS::SSM::ManagedInstanceInventory

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei), Kanada Barat (Calgary)

Parameter:

applicationNames, Jenis: CSV

Daftar nama aplikasi yang dipisahkan koma. Secara opsional, tentukan versi yang ditambahkan dengan ':' (misalnya, 'Chrome:0.5.3, Firefox').

> **Note**
>
> Nama aplikasi harus sama persis. Misalnya, gunakan **`firefox`** di Linux atau **`firefox-compat`** di Amazon Linux. Selain itu, saat ini AWS Config tidak mendukung wildcard untuk parameter ApplicationNames (misalnya,). **`firefox*`**

PlatformType (Opsional), Tipe: String

Jenis platform (misalnya, 'Linux' atau 'Windows').

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ec2- -periksa managedinstance-association-compliance-status

Memeriksa apakah status kepatuhan asosiasi AWS Systems Manager adalah COMPLIANT atau NON_COMPLIANT setelah eksekusi asosiasi pada instance. Aturannya sesuai jika status bidang COMPLIANT. Untuk informasi lebih lanjut tentang asosiasi, lihat Apa itu asosiasi? .

Pengidentifikasi: EC2 _MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK

Jenis Sumber Daya: AWS::SSM::AssociationCompliance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Afrika (Cape Town), Asia Pasifik (Hyderabad), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Eropa (Milan), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ec2- managedinstance-inventory-blacklisted

Memeriksa apakah instans yang dikelola oleh Amazon EC2 Systems Manager dikonfigurasi untuk mengumpulkan jenis inventaris yang masuk daftar hitam.

Pengidentifikasi: EC2 _MANAGEDINSTANCE_INVENTORY_BLACKLISTED

Jenis Sumber Daya: AWS::SSM::ManagedInstanceInventory

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei), Kanada Barat (Calgary)

Parameter:

inventoryNames, Jenis: CSV

Daftar tipe inventaris Systems Manager yang dipisahkan koma (misalnya, ':Network AWS,: AWS'). WindowsUpdate

PlatformType (Opsional), Tipe: String

Jenis platform (misalnya, 'Linux').

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ec2- -periksa managedinstance-patch-compliance-status

Memeriksa apakah status kepatuhan kepatuhan patch AWS Systems Manager adalah COMPLIANT atau NON_COMPLIANT setelah instalasi patch pada instance. Aturannya sesuai jika status bidang COMPLIANT.

Pengidentifikasi: EC2 _MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK

Jenis Sumber Daya: AWS::SSM::PatchCompliance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Osaka), Eropa (Milan), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ec2- managedinstance-platform-check

Memeriksa apakah instance EC2 terkelola memiliki konfigurasi yang diinginkan.

Pengidentifikasi: EC2 _MANAGEDINSTANCE_PLATFORM_CHECK

Jenis Sumber Daya: AWS::SSM::ManagedInstanceInventory

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei), Kanada Barat (Calgary)

Parameter:

platformType, Tipe: String

Jenis platform (misalnya, 'Linux').

PlatformVersion (Opsional), Tipe: String

Versi platform (misalnya, '2016.09').

AgentVersion (Opsional), Tipe: String

Versi agen (misalnya, '2.0.433.0').

PlatformName (Opsional), Tipe: String

Versi platform (misalnya, '2016.09')

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ec2- meets-restore-time-target

Memeriksa apakah waktu pemulihan instans Amazon Elastic Compute Cloud (Amazon EC2) memenuhi durasi yang ditentukan. Aturannya adalah NON_COMPLIANT jika LatestRestoreExecutionTimeMinutes EC2 instance Amazon lebih besar dari menit. maxRestoreTime

Pengidentifikasi: EC2 _MEETS_RESTORE_TIME_TARGET

Jenis Sumber Daya: AWS::EC2::Instance

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

maxRestoreTime, Jenis: int

Nilai numerik untuk runtime pemulihan maksimum yang diizinkan.

ResourceTags (Opsional), Tipe: String

Tag EC2 instans Amazon untuk aturan yang akan diperiksa, dalam format JSON.

ResourceID (Opsional), Tipe: String

ID EC2 instans Amazon untuk aturan yang akan diperiksa.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ec2- network-insights-access-scope -analisis ditandai

Memeriksa apakah analisis cakupan akses wawasan EC2 jaringan Amazon memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: EC2 _NETWORK_INSIGHTS_ACCESS_SCOPE_ANALYSIS_TAGGED

Jenis Sumber Daya: AWS::EC2::NetworkInsightsAccessScopeAnalysis

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah),

Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ec2- -ditandai network-insights-access-scope

Memeriksa apakah cakupan akses wawasan EC2 jaringan Amazon memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: EC2 _NETWORK_INSIGHTS_ACCESS_SCOPE_TAGGED

Jenis Sumber Daya: AWS::EC2::NetworkInsightsAccessScope

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ec2- network-insights-path-tagged

Memeriksa apakah jalur wawasan EC2 jaringan Amazon memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: EC2 _NETWORK_INSIGHTS_PATH_TAGGED

Jenis Sumber Daya: AWS::EC2::NetworkInsightsPath

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ec2- no-amazon-key-pair

Memeriksa apakah menjalankan instans Amazon Elastic Compute Cloud (EC2) diluncurkan menggunakan pasangan kunci amazon. Aturannya adalah NON_COMPLIANT jika EC2 instance yang sedang berjalan diluncurkan dengan key pair.

Pengidentifikasi: EC2 _NO_AMAZON_KEY_PAIR

Jenis Sumber Daya: AWS::EC2::Instance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ec2- paravirtual-instance-check

Memeriksa apakah jenis virtualisasi dari sebuah EC2 instance adalah paravirtual. Aturan ini adalah NON_COMPLIANT untuk sebuah EC2 instance jika 'VirtualizationType' disetel ke 'paravirtual'.

Pengidentifikasi: EC2 _PARAVIRTUAL_INSTANCE_CHECK

Jenis Sumber Daya: AWS::EC2::Instance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Tiongkok (Beijing), Eropa (Irlandia), Eropa (Frankfurt), Amerika Selatan (Sao Paulo), AS Timur (Virginia N.), Asia Pasifik (Tokyo), AS Barat (Oregon), AS Barat (California N.), Asia Pasifik (Singapura), Wilayah Asia Pasifik (Sydney)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ec2- prefix-list-tagged

Memeriksa apakah daftar awalan EC2 terkelola Amazon memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk aturan tersebut. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: EC2 _PREFIX_LIST_TAGGED

Jenis Sumber Daya: AWS::EC2::PrefixList

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ec2- resources-in-logically-air -gapped-lemari besi

Memeriksa apakah instans Amazon Elastic Compute Cloud (Amazon EC2) berada dalam brankas yang memiliki gap udara secara logis. Aturannya adalah NON_COMPLIANT EC2 jika instance Amazon tidak berada dalam brankas yang memiliki gap udara secara logis dalam periode waktu yang ditentukan.

Pengidentifikasi: EC2 _RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

Jenis Sumber Daya: AWS::EC2::Instance

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

ResourceTags (Opsional), Tipe: String

Tag EC2 instans Amazon untuk aturan yang akan diperiksa, dalam format JSON.

ResourceID (Opsional), Tipe: String

ID EC2 instans Amazon untuk aturan yang akan diperiksa.

recoveryPointAgeNilai (Opsional), Jenis: int, Default: 1

Nilai numerik untuk usia maksimum yang diizinkan. Tidak lebih dari 2184 jam, 91 untuk hari.

recoveryPointAgeUnit (Opsional), Tipe: String, Default: hari

Satuan waktu untuk usia maksimum yang diizinkan. Nilai yang diterima: 'jam', 'hari'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ec2- -rencana resources-protected-by-backup

Memeriksa apakah instans Amazon Elastic Compute Cloud (Amazon EC2) dilindungi oleh paket cadangan. Aturannya adalah NON_COMPLIANT EC2 jika instans Amazon tidak dicakup oleh paket cadangan.

> **Note**
>
> Aturan ini hanya berlaku untuk menjalankan EC2 instans Amazon dan bukan untuk instans yang dimatikan.

Pengidentifikasi: EC2 _RESOURCES_PROTECTED_BY_BACKUP_PLAN

Jenis Sumber Daya: AWS::EC2::Instance

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

ResourceTags (Opsional), Tipe: String

Tag untuk EC2 instans Amazon untuk aturan yang akan diperiksa, dalam format JSON. `{"tagkey" : "tagValue"}`

ResourceID (Opsional), Tipe: String

ID EC2 instans Amazon untuk aturan yang akan diperiksa.

crossRegionList (Opsional), Tipe: String

Daftar wilayah tujuan yang dipisahkan koma untuk salinan cadangan lintas wilayah yang akan disimpan

crossAccountList (Opsional), Tipe: String

Daftar akun tujuan yang dipisahkan koma untuk salinan cadangan lintas akun yang akan disimpan

maxRetentionDays (Opsional), Jenis: int

Periode retensi maksimum dalam beberapa hari untuk Backup Vault Lock

minRetentionDays (Opsional), Jenis: int

Periode retensi minimum dalam beberapa hari untuk Backup Vault Lock

backupVaultLockPeriksa (Opsional), Tipe: String

Nilai yang diterima: 'Benar' atau 'False'. Masukkan 'Benar' untuk aturan untuk memeriksa apakah sumber daya dicadangkan di brankas yang terkunci

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ec2- -eni security-group-attached-to

Memeriksa apakah grup keamanan non-default dilampirkan ke antarmuka jaringan elastis. Aturannya adalah NON_COMPLIANT jika grup keamanan tidak terkait dengan antarmuka jaringan.

Pengidentifikasi: EC2 _SECURITY_GROUP_ATTACHED_TO_ENI

Jenis Sumber Daya: AWS::EC2::SecurityGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (UEA), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ec2- security-group-attached-to -eni-periodik

Memeriksa apakah grup keamanan non-default dilampirkan ke antarmuka jaringan Elastis ()ENIs. Aturannya adalah NON_COMPLIANT jika grup keamanan tidak terkait dengan ENI. Grup keamanan yang tidak dimiliki oleh akun panggilan mengevaluasi sebagai NOT_APPLICABLE.

> **Note**
>
> Aturan ini melaporkan jenis `AWS::EC2::SecurityGroup` sumber daya. Namun, agar aturan berjalan secara efektif, Anda harus mengaktifkan perekaman jenis `AWS::EC2::NetworkInterface` sumber daya.

Pengidentifikasi: EC2 _SECURITY_GROUP_ATTACHED_TO_ENI_PERIODIC

Jenis Sumber Daya: AWS::EC2::SecurityGroup

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ec2- - spot-fleet-request-ct encryption-at-rest

Memeriksa apakah permintaan Amazon EC2 Spot Fleet telah mengenkripsi volume Amazon Elastic Block Store (Amazon EBS) untuk semua instans yang diluncurkan. EC2 Aturannya adalah NON_COMPLIANT jika salah satu volume EBS tidak dienkripsi saat istirahat.

Pengidentifikasi: EC2 _SPOT_FLEET_REQUEST_CT_ENCRYPTION_AT_REST

Jenis Sumber Daya: AWS::EC2::SpotFleet

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Eropa (Irlandia), AS Timur (Virginia N.), Asia Pasifik (Seoul), AS Barat (Oregon), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ec2-stopped-instance

Memeriksa apakah ada instans Amazon Elastic Compute Cloud (Amazon EC2) yang dihentikan selama lebih dari jumlah hari yang diizinkan. Aturannya adalah NON_COMPLIANT jika status EC2 instans Amazon telah dihentikan lebih lama dari jumlah hari yang diizinkan, atau jika jumlah waktu tidak dapat ditentukan.

Pengidentifikasi: EC2 _STOPPED_INSTANCE

Jenis Sumber Daya: AWS::EC2::Instance

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Afrika (Cape Town), Timur Tengah (UEA), Asia Pasifik (Osaka), Asia Pasifik (Melbourne), Eropa (Milan), Wilayah Kanada Barat (Calgary)

Parameter:

AllowedDays (Opsional), Jenis: int, Bawaan: 30

> Jumlah hari EC2 instans Amazon dapat dihentikan sebelum aturan NON_COMPLIANT. Jumlah hari default adalah 30.

> **Note**
>
> Jumlah hari yang dipilih harus kurang dari periode retensi yang dikonfigurasi karena aturan ini bergantung pada data historis yang dikumpulkan. Untuk informasi selengkapnya tentang retensi data historis, lihat Menghapus AWS Config Data.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ec2- token-hop-limit-check

Memeriksa apakah metadata instans Amazon Elastic Compute Cloud (EC2) memiliki batas token hop tertentu yang berada di bawah batas yang diinginkan. Aturannya adalah NON_COMPLIANT untuk sebuah instance jika memiliki nilai batas hop di atas batas yang dimaksud.

Pengidentifikasi: EC2 _TOKEN_HOP_LIMIT_CHECK

Jenis Sumber Daya: AWS::EC2::Instance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

tokenHopLimit (Opsional), Jenis: int

> Batas token hop yang diinginkan. Nilai yang valid adalah antara 1 dan 64, keduanya inklusif. Nilai default adalah 1 jika parameter tidak ditentukan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ec2- traffic-mirror-filter-description

Memeriksa apakah filter cermin EC2 lalu lintas Amazon memiliki deskripsi. Aturannya adalah NON_COMPLIANT jika Configuration.description tidak ada.

Pengidentifikasi: _TRAFFIC_MIROR_FILTER_DESCRIPTION EC2

Jenis Sumber Daya: AWS::EC2::TrafficMirrorFilter

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ec2- traffic-mirror-filter-tagged

Memeriksa apakah filter cermin EC2 lalu lintas Amazon memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk aturan tersebut. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: EC2 _TRAFFIC_MIROR_FILTER_TAGGED

Jenis Sumber Daya: AWS::EC2::TrafficMirrorFilter

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ec2- traffic-mirror-session-description

Memeriksa apakah sesi cermin EC2 lalu lintas Amazon memiliki deskripsi. Aturannya adalah NON_COMPLIANT jika Configuration.description tidak ada.

Pengidentifikasi: _TRAFFIC_MIROR_SESSION_DESCRIPTION EC2

Jenis Sumber Daya: AWS::EC2::TrafficMirrorSession

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Afrika (Cape Town), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Eropa (Milan), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ec2- traffic-mirror-session-tagged

Memeriksa apakah sesi cermin EC2 lalu lintas Amazon memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk aturan tersebut. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: EC2 _TRAFFIC_MIROR_SESSION_TAGGED

Jenis Sumber Daya: AWS::EC2::TrafficMirrorSession

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Afrika (Cape Town), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Eropa (Milan), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Tiongkok (Ningxia)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ec2- traffic-mirror-target-description

Memeriksa apakah target mirror EC2 lalu lintas Amazon memiliki deskripsi. Aturannya adalah NON_COMPLIANT jika Configuration.description tidak ada.

Pengidentifikasi: _TRAFFIC_MIROR_TARGET_DESCRIPTION EC2

Jenis Sumber Daya: AWS::EC2::TrafficMirrorTarget

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Afrika (Cape Town), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ec2- traffic-mirror-target-tagged

Memeriksa apakah target mirror EC2 lalu lintas Amazon memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk aturan tersebut. Aturannya adalah NON_COMPLIANT jika tidak ada tag

atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: EC2 _TRAFFIC_MIROR_TARGED_TAGGED

Jenis Sumber Daya: AWS::EC2::TrafficMirrorTarget

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Afrika (Cape Town), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Tiongkok (Ningxia)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan

Memeriksa apakah Gateway Transit Amazon Elastic Compute Cloud (Amazon EC2) telah 'AutoAcceptSharedAttachmentsdiaktifkan. Aturannya adalah NON_COMPLIANT untuk Transit Gateway jika '' disetel ke AutoAcceptSharedAttachments 'aktifkan'.

Pengidentifikasi: _TRANSIT_GATEWAY_AUTO_VPC_ATTACH_DISABLED EC2

Jenis Sumber Daya: AWS::EC2::TransitGateway

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud ,

(AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ec2- -ditandai transit-gateway-multicast-domain

Memeriksa apakah domain multicast gateway EC2 transit Amazon memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: EC2 _TRANSIT_GATEWAY_MULTICAST_DOMAIN_TAGGED

Jenis Sumber Daya: AWS::EC2::TransitGatewayMulticastDomain

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ec2- volume-inuse-check

Memeriksa apakah volume EBS dilampirkan ke EC2 instance. Secara opsional memeriksa apakah volume EBS ditandai untuk dihapus ketika sebuah instance dihentikan.

Aturannya adalah COMPLIANT jika volume EBS dilampirkan ke instance yang sedang berjalan EC2 . Dalam hal ini, itu adalah COMPLIANT ketika volume EBS secara aktif digunakan oleh sebuah EC2 instance.

Aturannya adalah NON_COMPLIANT jika volume EBS tidak dilampirkan ke EC2 instance apa pun atau dilampirkan ke instance yang dihentikan atau dihentikan. EC2 Dalam hal ini, adalah NON_COMPLIANT ketika volume EBS tidak aktif digunakan oleh sebuah instance. EC2

Pengidentifikasi: EC2 _VOLUME_INUSE_CHECK

Jenis Sumber Daya: AWS::EC2::Volume

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei), Kanada Barat (Calgary)

Parameter:

deleteOnTermination (Opsional), Jenis: boolean

> Volume EBS ditandai untuk dihapus ketika sebuah instance dihentikan. Nilai yang mungkin: Benar atau Salah (nilai input lainnya ditandai sebagai NON_COMPLIANT). Jika disetel ke`True`, aturannya adalah NON_COMPLIANT jika volume EBS yang dihentikan tidak ditandai untuk dihapus.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ec2- vpn-connection-logging-enabled

Memeriksa apakah koneksi AWS Site-to-Site VPN mengaktifkan CloudWatch pencatatan Amazon untuk kedua terowongan. Aturannya adalah NON_COMPLIANT jika koneksi Site-to-Site VPN tidak mengaktifkan CloudWatch logging untuk salah satu atau kedua terowongan.

Pengidentifikasi: _VPN_CONNECTION_LOGGING_ENABLED EC2

Jenis Sumber Daya: AWS::EC2::VPNConnection

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ecr-private-image-scanning-diaktifkan

Memeriksa apakah repositori Amazon Elastic Container Registry (Amazon ECR) pribadi mengaktifkan pemindaian gambar. Aturannya adalah NON_COMPLIANT jika frekuensi pemindaian repositori Amazon ECR pribadi tidak sedang dipindai saat push atau pemindaian berkelanjutan. Untuk informasi selengkapnya tentang mengaktifkan pemindaian gambar, lihat Pemindaian gambar di Panduan Pengguna Amazon ECR.

Pengidentifikasi: ECR_PRIVATE_IMAGE_SCANNING_ENABLED

Jenis Sumber Daya: AWS::ECR::Repository

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ecr-private-lifecycle-policy-dikonfigurasi

Memeriksa apakah repositori Amazon Elastic Container Registry (ECR) pribadi memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi. Aturannya adalah NON_COMPLIANT jika tidak ada kebijakan siklus hidup yang dikonfigurasi untuk repositori pribadi ECR.

Pengidentifikasi: ECR_PRIVATE_LIFECYCLE_POLICY_CONFIGURATED

Jenis Sumber Daya: AWS::ECR::Repository

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ecr-private-tag-immutability-diaktifkan

Memeriksa apakah repositori Amazon Elastic Container Registry (ECR) pribadi telah mengaktifkan kekekalan tag. Aturan ini NON_COMPLIANT jika kekekalan tag tidak diaktifkan untuk repositori ECR pribadi.

Pengidentifikasi: ECR_PRIVATE_TAG_IMMUTABILITY_ENABLED

Jenis Sumber Daya: AWS::ECR::Repository

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ecr-repository-cmk-encryption-diaktifkan

Memeriksa apakah repositori ECR dienkripsi saat istirahat menggunakan kunci KMS yang dikelola pelanggan. Aturan ini NON_COMPLIANT jika repositori dienkripsi menggunakan AES256 atau kunci KMS default ('aws/ecr').

Pengidentifikasi: ECR_REPOSITORY_CMK_ENCRYPTION_ENABLED

Jenis Sumber Daya: AWS::ECR::Repository

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (Bahrain), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

kmsKeyArns (Opsional), Jenis: CSV

> Daftar kunci KMS yang dipisahkan koma Amazon Resource Names (ARNs) dimaksudkan untuk mengenkripsi repositori ECR.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ecr-repository-tagged

Memeriksa apakah repositori Amazon ECR memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: ECR_REPOSITORY_TAGGED

Jenis Sumber Daya: AWS::ECR::Repository

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ecs-awsvpc-networking-enabled

Memeriksa apakah mode jaringan untuk ECSTask Definisi aktif diatur ke 'awsvpc'. Aturan ini NON_COMPLIANT jika ECSTask Definisi aktif tidak disetel ke 'awsvpc'.

> **Note**
>
> Aturan ini hanya mengevaluasi revisi aktif terbaru dari definisi tugas Amazon ECS.

Pengidentifikasi: AWSVPC_NETWORKING ECS_ _DIAKTIFKAN

Jenis Sumber Daya: AWS::ECS::TaskDefinition

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ecs-containers-nonprivileged

Memeriksa apakah parameter istimewa dalam definisi kontainer ECSTask Definisi diatur ke 'benar'. Aturannya adalah NON_COMPLIANT jika parameter istimewa adalah 'benar'.

> **Note**
>
> Aturan ini hanya mengevaluasi revisi aktif terbaru dari definisi tugas Amazon ECS.

Pengidentifikasi: ECS_CONTAINERS_NONPRIVILEGED

Jenis Sumber Daya: AWS::ECS::TaskDefinition

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ecs-containers-readonly-access

Memeriksa apakah Amazon Elastic Container Service (Amazon ECS) Container hanya memiliki akses read-only ke sistem file root. Aturannya adalah NON_COMPLIANT jika readonlyRootFilesystem parameter dalam definisi kontainer Definisi disetel ke ECSTask 'false'.

> **Note**
>
> Aturan ini hanya mengevaluasi revisi aktif terbaru dari definisi tugas Amazon ECS.

Pengidentifikasi: ECS_CONTAINERS_READONLY_ACCESS

Jenis Sumber Daya: AWS::ECS::TaskDefinition

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ecs-container-insights-enabled

Memeriksa apakah klaster Amazon Elastic Container Service mengaktifkan wawasan kontainer. Aturannya adalah NON_COMPLIANT jika wawasan kontainer tidak diaktifkan.

Pengidentifikasi: ECS_CONTAINER_INSIGHTS_ENABLED

Jenis Sumber Daya: AWS::ECS::Cluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ecs-fargate-latest-platform-versi

Memeriksa apakah layanan ECS Fargate diatur ke versi platform terbaru. Aturannya adalah NON_COMPLIANT jika PlatformVersion untuk jenis peluncuran Fargate tidak disetel ke TERBARU, atau jika tidak ada latestLinuxVersion atau `latestWindowsVersion` disediakan sebagai parameter.

Pengidentifikasi: ECS_FARGATE_LATEST_PLATFORM_VERSION

Jenis Sumber Daya: AWS::ECS::Service

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

latestLinuxVersion (Opsional), Tipe: String

> Linux terbaru mendukung 'PlatformVersion' dalam format versi semantik (). SemVer Parameter mungkin diperlukan jika Fargate digunakan dan 'PlatformVersion' secara eksplisit ditentukan atau CodeDeploy digunakan sebagai '' DeploymentController

latestWindowsVersion (Opsional), Tipe: String

Windows terbaru mendukung 'PlatformVersion' dalam format versi semantik (). SemVer Parameter mungkin diperlukan jika Fargate digunakan dan 'PlatformVersion' secara eksplisit ditentukan atau CodeDeploy digunakan sebagai '' DeploymentController

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ecs-no-environment-secrets

Memeriksa apakah rahasia diteruskan sebagai variabel lingkungan kontainer. Aturannya adalah NON_COMPLIANT jika 1 atau lebih kunci variabel lingkungan cocok dengan kunci yang tercantum dalam parameter '`secretKeys`' (tidak termasuk variabel lingkungan dari lokasi lain seperti Amazon S3).

> **Note**
> Aturan ini hanya mengevaluasi revisi aktif terbaru dari definisi tugas Amazon ECS.

Pengidentifikasi: ECS_NO_ENVIRONMENT_SECRETS

Jenis Sumber Daya: AWS::ECS::TaskDefinition

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), AWS GovCloud (AS-Timur), AWS GovCloud (AS-Barat), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

SecretKeys, Jenis: CSV

Daftar nama kunci yang dipisahkan koma untuk dicari dalam variabel lingkungan definisi wadah dalam Definisi Tugas. Ruang ekstra akan dihapus.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ecs-task-definition-log-konfigurasi

Memeriksa apakah LogConfiguration diatur pada Definisi Tugas ECS aktif. Aturan ini NON_COMPLIANT jika ECSTask Definisi aktif tidak memiliki sumber daya LogConfiguration yang ditentukan atau nilai untuk LogConfiguration adalah null dalam setidaknya satu definisi kontainer.

> **Note**
>
> Aturan ini hanya mengevaluasi revisi aktif terbaru dari definisi tugas Amazon ECS.

Pengidentifikasi: ECS_TASK_DEFINITION_LOG_CONFIGURATION

Jenis Sumber Daya: AWS::ECS::TaskDefinition

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), AWS GovCloud (AS-Timur), AWS GovCloud (AS-Barat), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ecs-task-definition-memory-batas-keras

Memeriksa apakah definisi tugas Amazon Elastic Container Service (ECS) memiliki batas memori yang ditetapkan untuk definisi kontainernya. Aturannya adalah NON_COMPLIANT untuk definisi tugas jika parameter 'memori' tidak ada untuk satu definisi kontainer.

> **Note**
>
> Aturan ini hanya mengevaluasi revisi aktif terbaru dari definisi tugas Amazon ECS.

Pengidentifikasi: ECS_TASK_DEFINITION_MEMORY_HARD_LIMIT

Jenis Sumber Daya: AWS::ECS::TaskDefinition

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ecs-task-definition-network-mode-not-host

Memeriksa apakah revisi aktif terbaru dari definisi tugas Amazon ECS menggunakan mode jaringan host. Aturannya adalah NON_COMPLIANT jika revisi aktif terbaru dari definisi tugas ECS menggunakan mode jaringan host.

Pengidentifikasi: ECS_TASK_DEFINITION_NETWORK_MODE_NOT_HOST

Jenis Sumber Daya: AWS::ECS::TaskDefinition

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (Bahrain), Asia Pasifik (Thailand), Meksiko (Tengah), Wilayah Asia Pasifik (Taipei)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ecs-task-definition-nonroot-pengguna

Memeriksa apakah ECSTask Definisi menentukan pengguna untuk container tipe peluncuran Amazon Elastic Container Service (Amazon EC2 ECS) untuk dijalankan. Aturannya adalah NON_COMPLIANT jika parameter 'pengguna' tidak ada atau disetel ke 'root'.

> **Note**
>
> Aturan ini hanya mengevaluasi revisi aktif terbaru dari definisi tugas Amazon ECS.

Pengidentifikasi: ECS_TASK_DEFINITION_NONROOT_USER

Jenis Sumber Daya: AWS::ECS::TaskDefinition

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ecs-task-definition-pid-mode-periksa

Memeriksa apakah ECSTask Definisi dikonfigurasi untuk berbagi namespace proses host dengan wadah Amazon Elastic Container Service (Amazon ECS). Aturannya adalah NON_COMPLIANT jika parameter PidMode disetel ke 'host'.

> **Note**
>
> Aturan ini hanya mengevaluasi revisi aktif terbaru dari definisi tugas Amazon ECS.

Pengidentifikasi: ECS_TASK_DEFINITION_PID_MODE_CHECK

Jenis Sumber Daya: AWS::ECS::TaskDefinition

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), AWS GovCloud (AS-Timur), AWS GovCloud (AS-Barat), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ecs-task-definition-user-for-host-mode-check

Memeriksa apakah definisi tugas Amazon ECS dengan mode jaringan host memiliki hak istimewa ATAU nonroot dalam definisi penampung. Aturannya adalah NON_COMPLIANT jika revisi aktif terbaru dari definisi tugas memiliki privileged=false (atau null) DAN user=root (atau null).

> **Important**
>
> Hanya satu syarat yang harus dipenuhi agar aturan dapat kembali sesuai
> Aturannya SESUAI dalam salah satu skenario berikut:

- Jika mode jaringan tidak diatur ke host,
- Jika revisi aktif terbaru dari definisi tugas memiliki privileged=true,
- Jika revisi aktif terbaru dari definisi tugas memiliki pengguna yang bukan root.

Ini berarti bahwa hanya satu dari kondisi ini yang perlu dipenuhi agar aturan dapat kembali sesuai. Untuk memeriksa secara spesifik apakah definisi tugas memiliki privileged=true, lihat. ecs-containers-nonprivileged Untuk memeriksa secara spesifik apakah definisi tugas memiliki pengguna yang bukan root, lihat ecs-task-definition-nonroot-user.

Pengidentifikasi: ECS_TASK_DEFINITION_USER_FOR_HOST_MODE_CHECK

Jenis Sumber Daya: AWS::ECS::TaskDefinition

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Timur Tengah (UEA), Asia Pasifik (Taipei)

Parameter:

SkipInactiveTaskDefinitions (Opsional), Jenis: boolean

Boolean flag untuk tidak memeriksa definisi EC2 tugas Amazon INACTIVE. Jika disetel ke 'true', aturan tidak akan mengevaluasi definisi EC2 tugas Amazon INACTIVE. Jika disetel ke 'false', aturan akan mengevaluasi revisi terbaru dari definisi EC2 tugas Amazon INACTIVE.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

efs-access-point-enforce-root-direktori

Memeriksa apakah titik akses Amazon Elastic File System (Amazon EFS) dikonfigurasi untuk menerapkan direktori root. Aturannya adalah NON_COMPLIANT jika nilai 'Path' diatur ke '/' (direktori root default dari sistem file).

Pengidentifikasi: EFS_ACCESS_POINT_ENFORCE_ROOT_DIRECTORY

Jenis Sumber Daya: AWS::EFS::AccessPoint

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur), AWS GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

ApprovedDirectories (Opsional), Jenis: CSV

> Daftar jalur subdirektori yang dipisahkan koma yang disetujui untuk penegakan direktori root titik akses Amazon EFS.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

efs-access-point-enforce-identitas pengguna

Memeriksa apakah titik akses Amazon Elastic File System (Amazon EFS) dikonfigurasi untuk menegakkan identitas pengguna. Aturannya adalah NON_COMPLIANT jika PosixUser '' tidak ditentukan atau jika parameter disediakan dan tidak ada kecocokan dalam parameter yang sesuai.

Pengidentifikasi: EFS_ACCESS_POINT_ENFORCE_USER_IDENTITY

Jenis Sumber Daya: AWS::EFS::AccessPoint

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

ApproveDuids (Opsional), Jenis: CSV

> Daftar ID pengguna POSIX yang dipisahkan koma yang disetujui untuk penegakan pengguna titik akses EFS.

ApprovedGIDS (Opsional), Jenis: CSV

Daftar grup POSIX yang dipisahkan koma IDs yang disetujui untuk penegakan pengguna titik akses EFS.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

efs-automatic-backups-enabled

Memeriksa apakah sistem file Amazon Elastic File System (Amazon EFS) mengaktifkan pencadangan otomatis. Aturannya adalah NON_COMPLIANT jika `BackupPolicy.Status` disetel ke DISABLED.

Pengidentifikasi: EFS_AUTOMATIC_BACKUPS_ENABLED

Jenis Sumber Daya: AWS::EFS::FileSystem

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

efs-encrypted-check

Memeriksa apakah Amazon Elastic File System (Amazon EFS) dikonfigurasi untuk mengenkripsi data file menggunakan AWS Key Management Service (AWS KMS). Aturannya adalah NON_COMPLIANT jika kunci terenkripsi disetel ke false on `DescribeFileSystems` atau jika `KmsKeyId` kunci aktif `DescribeFileSystems` tidak cocok dengan parameter. `KmsKeyId`

Pengidentifikasi: EFS_ENCRYPTED_CHECK

Jenis Sumber Daya: AWS::EFS::FileSystem

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei)

Parameter:

KmsKeyId (Opsional), Tipe: String

> Amazon Resource Name (ARN) dari kunci KMS yang digunakan untuk mengenkripsi sistem file EFS.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

efs-filesystem-ct-encrypted

Memeriksa apakah Amazon Elastic File System (Amazon EFS) mengenkripsi data dengan AWS Key Management Service (AWS KMS). Aturannya adalah NON_COMPLIANT jika sistem file tidak dienkripsi. Secara opsional, Anda dapat memeriksa apakah sistem file tidak dienkripsi dengan kunci KMS tertentu.

Pengidentifikasi: EFS_FILESYSTEM_CT_ENCRYPTED

Jenis Sumber Daya: AWS::EFS::FileSystem

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

kmsKeyArns (Opsional), Tipe: String

> (Opsional) Daftar Nama Sumber Daya Amazon (ARNs) yang dipisahkan koma untuk kunci AWS KMS. Jika disediakan, aturan akan memeriksa apakah kunci KMS yang ditentukan tidak mengenkripsi sistem file Amazon EFS.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

efs-in-backup-plan

Memeriksa apakah sistem file Amazon Elastic File System (Amazon EFS) ditambahkan dalam paket cadangan AWS Backup. Aturannya adalah NON_COMPLIANT jika sistem file EFS tidak disertakan dalam paket cadangan.

Pengidentifikasi: EFS_IN_BACKUP_PLAN

Jenis Sumber Daya: AWS::EFS::FileSystem

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

efs-last-backup-recovery-point-dibuat

Memeriksa apakah titik pemulihan dibuat untuk Sistem File Amazon Elastic File System (Amazon EFS). Aturannya adalah NON_COMPLIANT jika Sistem File Amazon EFS tidak memiliki Titik Pemulihan terkait yang dibuat dalam periode waktu yang ditentukan.

Pengidentifikasi: EFS_LAST_BACKUP_RECOVERY_POINT_CREATED

Jenis Sumber Daya: AWS::EFS::FileSystem

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

ResourceTags (Opsional), Tipe: String

Tag Sistem File Amazon EFS untuk aturan yang akan diperiksa, dalam format `{"tagkey" : "tagValue"}` JSON.

ResourceID (Opsional), Tipe: String

ID Sistem File EFS untuk aturan yang akan diperiksa.

recoveryPointAgeNilai (Opsional), Jenis: int, Default: 1

Nilai numerik untuk usia maksimum yang diizinkan. Tidak lebih dari 744 jam, 31 untuk hari.

recoveryPointAgeUnit (Opsional), Tipe: String, Default: hari

Satuan waktu untuk usia maksimum yang diizinkan. Nilai yang diterima: 'jam', 'hari'.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

efs-meets-restore-time-target

Memeriksa apakah waktu pemulihan Sistem File Amazon Elastic File System (Amazon EFS) memenuhi durasi yang ditentukan. Aturannya adalah NON_COMPLIANT jika LatestRestoreExecutionTimeMinutes Sistem File Amazon EFS lebih besar dari menit. maxRestoreTime

Pengidentifikasi: EFS_MEETS_RESTORE_TIME_TARGET

Jenis Sumber Daya: AWS::EFS::FileSystem

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

maxRestoreTime, Jenis: int

Nilai numerik untuk runtime pemulihan maksimum yang diizinkan.

ResourceTags (Opsional), Tipe: String

Tag Amazon EFS File Systems untuk aturan yang akan diperiksa, dalam format JSON.

ResourceID (Opsional), Tipe: String

ID Sistem File EFS untuk aturan yang akan diperiksa.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

efs-mount-target-public-dapat diakses

Memeriksa apakah target pemasangan Amazon Elastic File System (Amazon EFS) tidak terkait dengan subnet publik. Aturannya adalah NON-COMPLIANT jika target pemasangan Amazon EFS dikaitkan dengan subnet publik.

Pengidentifikasi: EFS_MOUNT_TARGET_PUBLIC_ACCESSIBLE

Jenis Sumber Daya: AWS::EFS::FileSystem

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

efs-resources-in-logically-air-gapped-vault

Memeriksa apakah Sistem File Amazon Elastic File System (Amazon EFS) berada dalam brankas yang memiliki gapped udara secara logis. Aturannya adalah NON_COMPLIANT jika Sistem File Amazon EFS tidak berada dalam brankas dengan gapped udara secara logis dalam periode waktu yang ditentukan.

Pengidentifikasi: EFS_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

Jenis Sumber Daya: AWS::EFS::FileSystem

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

ResourceTags (Opsional), Tipe: String

Tag Amazon EFS File Systems untuk aturan yang akan diperiksa, dalam format JSON.

ResourceID (Opsional), Tipe: String

ID Sistem File EFS untuk aturan yang akan diperiksa.

recoveryPointAgeNilai (Opsional), Jenis: int, Default: 1

Nilai numerik untuk usia maksimum yang diizinkan. Tidak lebih dari 2184 jam, 91 untuk hari.

recoveryPointAgeUnit (Opsional), Tipe: String, Default: hari

Satuan waktu untuk usia maksimum yang diizinkan. Nilai yang diterima: 'jam', 'hari'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

efs-resources-protected-by-rencana cadangan

Memeriksa apakah Sistem File Amazon Elastic File System (Amazon EFS) dilindungi oleh paket cadangan. Aturannya adalah NON_COMPLIANT jika Sistem File EFS tidak dicakup oleh rencana cadangan.

Pengidentifikasi: EFS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Jenis Sumber Daya: AWS::EFS::FileSystem

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

ResourceTags (Opsional), Tipe: String

Tag untuk EFS File Systems untuk aturan yang akan diperiksa, dalam format `{"tagkey" : "tagValue"}` JSON.

ResourceID (Opsional), Tipe: String

ID Sistem File EFS untuk aturan yang akan diperiksa.

crossRegionList (Opsional), Tipe: String

Daftar wilayah tujuan yang dipisahkan koma untuk salinan cadangan lintas wilayah yang akan disimpan

crossAccountList (Opsional), Tipe: String

Daftar akun tujuan yang dipisahkan koma untuk salinan cadangan lintas akun yang akan disimpan

maxRetentionDays (Opsional), Jenis: int

Periode retensi maksimum dalam beberapa hari untuk Backup Vault Lock

minRetentionDays (Opsional), Jenis: int

Periode retensi minimum dalam beberapa hari untuk Backup Vault Lock

backupVaultLockPeriksa (Opsional), Tipe: String

Nilai yang diterima: 'Benar' atau 'False'. Masukkan 'Benar' untuk aturan untuk memeriksa apakah sumber daya dicadangkan di brankas yang terkunci

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

terlampir eip

Memeriksa apakah semua alamat IP Elastis yang dialokasikan ke AWS akun dilampirkan ke EC2 instance atau antarmuka jaringan elastis yang sedang digunakan. Aturannya adalah NON_COMPLIANT jika 'AssociationId' adalah null untuk alamat IP Elastis.

> **Note**
>
> Hasil mungkin memakan waktu hingga 6 jam untuk tersedia setelah evaluasi terjadi.

Pengidentifikasi: EIP_ATTACHED

Jenis Sumber Daya: AWS::EC2::EIP

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Timur Tengah (UEA)

Parameter:

Tidak ada

Evaluasi Proaktif

Untuk langkah-langkah tentang cara menjalankan aturan ini dalam mode proaktif, lihat Mengevaluasi Sumber Daya Anda dengan AWS Config Aturan. Agar aturan ini mengembalikan COMPLIANT dalam mode proaktif, skema konfigurasi sumber daya untuk StartResourceEvaluationAPI harus menyertakan input berikut, yang dikodekan sebagai string:

```
"ResourceConfiguration":
...
{
   "InstanceId": "my-instance-Id"
}
...
```

Untuk informasi lebih lanjut tentang evaluasi proaktif, lihat Mode Evaluasi.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

eks-cluster-logging-enabled

Memeriksa apakah klaster Amazon Elastic Kubernetes Service (Amazon EKS) dikonfigurasi dengan logging diaktifkan. Aturannya adalah NON_COMPLIANT jika logging untuk klaster Amazon EKS tidak diaktifkan untuk semua jenis log.

Pengidentifikasi: EKS_CLUSTER_LOGGING_ENABLED

Jenis Sumber Daya: AWS::EKS::Cluster

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

eks-cluster-log-enabled

Memeriksa apakah klaster Amazon Elastic Kubernetes Service (Amazon EKS) dikonfigurasi dengan logging diaktifkan. Aturannya adalah NON_COMPLIANT jika logging untuk kluster Amazon EKS tidak diaktifkan atau jika logging tidak diaktifkan dengan jenis log yang disebutkan.

Pengidentifikasi: EKS_CLUSTER_LOG_ENABLED

Jenis Sumber Daya: AWS::EKS::Cluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur), AWS GovCloud AWS GovCloud (AS-Barat), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary) Wilayah

Parameter:

LogTypes (Opsional), Jenis: CSV

> Daftar tipe log bidang kontrol EKS Cluster yang dipisahkan koma untuk diperiksa aturan. Nilai yang valid: “api”, “audit”, “authenticator”, “ControllerManager”, “scheduler

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

eks-cluster-oldest-supported-versi

Memeriksa apakah klaster Amazon Elastic Kubernetes Service (EKS) menjalankan versi tertua yang didukung. Aturannya adalah NON_COMPLIANT jika kluster EKS menjalankan versi tertua yang didukung (sama dengan parameter "`oldestVersionSupported`).

Pengidentifikasi: EKS_CLUSTER_OLDEST_SUPPORTED_VERSION

Jenis Sumber Daya: AWS::EKS::Cluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

oldestVersionSupported, Tipe: String

> Nilai dari versi tertua Kubernetes yang didukung pada. AWS

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

eks-cluster-secrets-encrypted

Memeriksa apakah klaster Amazon EKS dikonfigurasi agar rahasia Kubernetes dienkripsi menggunakan KMS. AWS Aturannya adalah NON_COMPLIANT jika kluster EKS tidak memiliki sumber daya EncryptionConfig atau jika EncryptionConfig tidak menyebutkan rahasia sebagai sumber daya.

Pengidentifikasi: EKS_CLUSTER_SECRETS_ENCRYPTED

Jenis Sumber Daya: AWS::EKS::Cluster

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

kmsKeyArns (Opsional), Jenis: CSV

> Daftar kunci KMS yang dipisahkan koma Nama Sumber Daya Amazon (ARNs) yang disetujui untuk penggunaan EKS.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

eks-cluster-supported-version

Memeriksa apakah klaster Amazon Elastic Kubernetes Service (EKS) menjalankan versi Kubernetes yang didukung. Aturan ini NON_COMPLIANT jika kluster EKS menjalankan versi yang tidak didukung (kurang dari parameter "). `oldestVersionSupported`

Pengidentifikasi: EKS_CLUSTER_SUPPORTED_VERSION

Jenis Sumber Daya: AWS::EKS::Cluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

oldestVersionSupported, Tipe: String

Nilai dari versi tertua Kubernetes yang didukung pada. AWS

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

eks-endpoint-no-public-akses

Memeriksa apakah titik akhir Amazon Elastic Kubernetes Service (Amazon EKS) tidak dapat diakses publik. Aturannya adalah NON_COMPLIANT jika titik akhir dapat diakses publik.

Pengidentifikasi: EKS_ENDPOINT_NO_PUBLIC_ACCESS

Jenis Sumber Daya: AWS::EKS::Cluster

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

eks-secrets-encrypted

Memeriksa apakah klaster Amazon Elastic Kubernetes Service dikonfigurasi agar rahasia Kubernetes dienkripsi menggunakan kunci (KMS). AWS Key Management Service

- Aturan ini SESUAI jika cluster EKS memiliki EncryptionConfig dengan rahasia sebagai salah satu sumber daya.
- Aturan ini juga COMPLIANT jika kunci yang digunakan untuk mengenkripsi rahasia EKS cocok dengan parameter.
- Aturan ini NON_COMPLIANT jika kluster EKS tidak memiliki EncryptionConfig atau jika sumber daya EncryptionConfig tidak menyertakan rahasia.
- Aturan ini juga NON_COMPLIANT jika kunci yang digunakan untuk mengenkripsi rahasia EKS tidak cocok dengan parameter.

Pengidentifikasi: EKS_SECRETS_ENCRYPTED

Jenis Sumber Daya: AWS::EKS::Cluster

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei)

Parameter:

kmsKeyArns (Opsional), Jenis: CSV

> Daftar dipisahkan koma dari Amazon Resource Name (ARN) dari kunci KMS yang harus digunakan untuk rahasia terenkripsi dalam kluster EKS.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

elasticache_automatic_backup_check_enabled

Memeriksa apakah ElastiCache cluster Amazon (Valkey atau Redis OSS) mengaktifkan cadangan otomatis. Aturannya adalah NON_COMPLIANT jika pencadangan otomatis tidak diaktifkan atau SnapshotRetentionLimit untuk klaster kurang dari yang ditentukan. `snapshotRetentionPeriod`

Pengidentifikasi: ELASTICACHE_AUTOMATIC_BACKUP_CHECK_ENABLED

Jenis Sumber Daya: AWS::ElastiCache::CacheCluster

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

snapshotRetentionPeriod (Opsional), Jenis: int

Periode retensi snapshot minimum dalam beberapa hari untuk Valkey atau Redis OSS. Nilai yang valid adalah 1 hingga 35. Nilai default adalah 1.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

elasticache-auto-minor-version-tingkatkan periksa

Memeriksa apakah ElastiCache kluster Amazon mengaktifkan peningkatan versi minor otomatis. Aturannya adalah NON_COMPLIANT untuk ElastiCache cluster jika menggunakan mesin Redis atau Valkey dan '' tidak disetel ke AutoMinorVersionUpgrade 'benar'.

Pengidentifikasi: ELASTICACHE_AUTO_MINOR_VERSION_UPGRADE_CHECK

Jenis Sumber Daya: AWS::ElastiCache::CacheCluster

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur), AWS GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

elasticache-rbac-auth-enabled

Memeriksa apakah grup ElastiCache replikasi Amazon mengaktifkan otentikasi RBAC. Aturannya adalah NON_COMPLIANT jika versi Redis 6 atau lebih tinggi dan 'UserGroupIds' hilang, kosong, atau tidak cocok dengan entri yang disediakan oleh parameter ". `allowedUserGroupIDs`

Pengidentifikasi: ELASTICACHE_RBAC_AUTH_ENABLED

Jenis Sumber Daya: AWS::ElastiCache::ReplicationGroup

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

allowedUserGroupIDs (Opsional), Jenis: CSV

> Daftar Grup Pengguna yang dipisahkan koma IDs yang disetujui untuk akses grup ElastiCache replikasi.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

elasticache-redis-cluster-automatic-backup-periksa

Periksa apakah kluster Amazon ElastiCache Redis mengaktifkan cadangan otomatis. Aturannya adalah NON_COMPLIANT jika cluster SnapshotRetentionLimit for Redis kurang dari parameter. SnapshotRetentionPeriod Misalnya: Jika parameternya 15 maka aturannya tidak sesuai jika antara snapshotRetentionPeriod 0-15.

Pengidentifikasi: ELASTICACHE_REDIS_CLUSTER_AUTOMATIC_BACKUP_CHECK

Jenis Sumber Daya: AWS::ElastiCache::CacheCluster, AWS::ElastiCache::ReplicationGroup

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei)

Parameter:

snapshotRetentionPeriod (Opsional), Jenis: int, Default: 15

> Periode retensi snapshot minimum dalam beberapa hari untuk klaster Redis. Default adalah 15 hari.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

elasticache-repl-grp-auto-failover-diaktifkan

Memeriksa apakah grup replikasi Amazon ElastiCache Redis mengaktifkan failover otomatis. Aturannya adalah NON_COMPLIANT untuk grup ElastiCache replikasi jika '' tidak disetel ke AutomaticFailover 'diaktifkan'.

Pengidentifikasi: ELASTICACHE_REPL_GRP_AUTO_FAILOVER_ENABLED

Jenis Sumber Daya: AWS::ElastiCache::ReplicationGroup

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur), AWS GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

elasticache-repl-grp-encrypted-saat istirahat

Memeriksa apakah grup ElastiCache replikasi Amazon telah encryption-at-rest diaktifkan. Aturannya adalah NON_COMPLIANT untuk grup ElastiCache replikasi jika 'AtRestEncryptionEnabled' dinonaktifkan atau jika ARN kunci KMS tidak cocok dengan parameter Arns yang disetujui. KMSKey

Pengidentifikasi: ELASTICACHE_REPL_GRP_ENCRYPTED_AT_REST

Jenis Sumber Daya: AWS::ElastiCache::ReplicationGroup

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur), AWS GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

KMSKeyID yang disetujui (Opsional), Jenis: CSV

Daftar KMS Key yang dipisahkan koma IDs yang disetujui untuk digunakan. ElastiCache

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

elasticache-repl-grp-encrypted-dalam transit

Memeriksa apakah grup ElastiCache replikasi Amazon telah encryption-in-transit diaktifkan. Aturannya adalah NON_COMPLIANT untuk grup ElastiCache replikasi jika '' disetel ke TransitEncryptionEnabled 'false'.

Pengidentifikasi: ELASTICACHE_REPL_GRP_ENCRYPTED_IN_TRANSIT

Jenis Sumber Daya: AWS::ElastiCache::ReplicationGroup

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur), AWS GovCloud (AS-Barat),

Meksiko AWS GovCloud (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

elasticache-repl-grp-redis-auth-diaktifkan

Memeriksa apakah grup ElastiCache replikasi Amazon mengaktifkan Redis AUTH. Aturannya adalah NON_COMPLIANT untuk grup ElastiCache replikasi jika versi Redis dari node-nya di bawah 6 (Versi 6+ menggunakan Redis ACLs) dan " AuthToken hilang atau kosong/null.

Pengidentifikasi: ELASTICACHE_REPL_GRP_REDIS_AUTH_ENABLED

Jenis Sumber Daya: AWS::ElastiCache::ReplicationGroup

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur), AWS GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

elasticache-subnet-group-check

Memeriksa apakah ElastiCache klaster Amazon dikonfigurasi dengan grup subnet khusus. Aturannya adalah NON_COMPLIANT untuk ElastiCache cluster jika menggunakan grup subnet default.

Pengidentifikasi: ELASTICACHE_SUBNET_GROUP_CHECK

Jenis Sumber Daya: AWS::ElastiCache::CacheCluster

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur), AWS GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

elasticache-supported-engine-version

Memeriksa apakah ElastiCache cluster menjalankan versi yang lebih besar atau sama dengan versi mesin yang direkomendasikan. Aturannya adalah NON_COMPLIANT jika 'EngineVersion' untuk ElastiCache cluster kurang dari versi yang direkomendasikan yang ditentukan untuk mesin yang diberikan.

Pengidentifikasi: ELASTICACHE_SUPPORTED_ENGINE_VERSION

Jenis Sumber Daya: AWS::ElastiCache::CacheCluster

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

latestMemcachedVersion, Tipe: String

Versi mesin terbaru yang direkomendasikan untuk Memcached. Nilai yang valid dalam format semantik versioning (SemVer) dengan nomor 3 komponen untuk versi mayor, minor, dan patch (misalnya, 1.6.6, bukan 1.6).

latestRedisVersion, Tipe: String

Versi mesin terbaru yang direkomendasikan untuk Redis. Nilai yang valid dalam format versi semantik (SemVer) dengan nomor 3 komponen untuk versi mayor, minor, dan patch (misalnya, 7.0.5, bukan 7.0).

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

elasticbeanstalk-application-description

Memeriksa apakah AWS aplikasi Elastic Beanstalk memiliki deskripsi. Aturannya adalah NON_COMPLIANT jika configuration.description tidak ada atau string kosong.

Pengidentifikasi: ELASTICBEANSTALK_APPLICATION_DESCRIPTION

Jenis Sumber Daya: AWS::ElasticBeanstalk::Application

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

elasticbeanstalk-application-version-description

Memeriksa apakah AWS versi aplikasi Elastic Beanstalk memiliki deskripsi. Aturannya adalah NON_COMPLIANT jika configuration.description tidak ada atau string kosong.

Pengidentifikasi: ELASTICBEANSTALK_APPLICATION_VERSION_DESCRIPTION

Jenis Sumber Daya: AWS::ElasticBeanstalk::ApplicationVersion

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

elasticbeanstalk-environment-description

Memeriksa apakah AWS lingkungan Elastic Beanstalk memiliki deskripsi. Aturannya adalah NON_COMPLIANT jika configuration.description tidak ada atau string kosong.

Pengidentifikasi: ELASTICBEANSTALK_ENVIRONMENT_DESCRIPTION

Jenis Sumber Daya: AWS::ElasticBeanstalk::Environment

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

elasticsearch-encrypted-at-rest

Memeriksa apakah domain Amazon OpenSearch Service (sebelumnya disebut Elasticsearch) mengaktifkan enkripsi saat konfigurasi istirahat. Aturannya adalah NON_COMPLIANT jika EncryptionAtRestOptions bidang tidak diaktifkan.

Pengidentifikasi: ELASTICSEARCH_ENCRYPTED_AT_REST

Jenis Sumber Daya: AWS::Elasticsearch::Domain

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

elasticsearch-in-vpc-only

Memeriksa apakah domain Amazon OpenSearch Service (sebelumnya disebut Elasticsearch) berada di Amazon Virtual Private Cloud (Amazon VPC). Aturannya adalah NON_COMPLIANT jika titik akhir domain OpenSearch Layanan bersifat publik.

Pengidentifikasi: ELASTICSEARCH_IN_VPC_ONLY

Jenis Sumber Daya: AWS::Elasticsearch::Domain

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

elasticsearch-logs-to-cloudwatch

Memeriksa apakah domain OpenSearch Layanan Amazon dikonfigurasi untuk mengirim log ke CloudWatch Log Amazon. Aturannya adalah COMPLIANT jika log diaktifkan untuk domain Amazon ES. Aturan ini adalah NON_COMPLIANT jika logging tidak dikonfigurasi.

Pengidentifikasi: ELASTICSEARCH_LOGS_TO_CLOUDWATCH

Jenis Sumber Daya: AWS::Elasticsearch::Domain

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei)

Parameter:

LogTypes (Opsional), Jenis: CSV

> Daftar log yang dipisahkan koma yang diaktifkan. Nilai yang valid adalah 'pencarian', 'indeks', 'kesalahan'.

Evaluasi Proaktif

Untuk langkah-langkah tentang cara menjalankan aturan ini dalam mode proaktif, lihat Mengevaluasi Sumber Daya Anda dengan AWS Config Aturan. Agar aturan ini mengembalikan COMPLIANT dalam mode proaktif, skema konfigurasi sumber daya untuk StartResourceEvaluationAPI harus menyertakan input berikut, yang dikodekan sebagai string:

```
"ResourceConfiguration":
...
```

```
{
   "LogPublishingOptions": "{Key : Value, ...}"*
}
...
```

* Objek dengan satu atau lebih kunci berikut:`SEARCH_SLOW_LOGS`,`ES_APPLICATION_LOGS`,`INDEX_SLOW_LOGS`,`AUDIT_LOGS`,, tergantung pada jenis log yang ingin Anda publikasikan. Setiap kunci membutuhkan nilai `LogPublishingOption` valid.

Untuk informasi lebih lanjut tentang evaluasi proaktif, lihat Mode Evaluasi.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

elasticsearch-node-to-node-pemeriksaan enkripsi-

Periksa apakah OpenSearch Service (sebelumnya disebut Elasticsearch) node dienkripsi ujung ke ujung. Aturannya adalah NON_COMPLIANT jika node-to-node enkripsi tidak diaktifkan pada domain.

Pengidentifikasi: ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

Jenis Sumber Daya: AWS::Elasticsearch::Domain

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei)

Parameter:

Tidak ada

Evaluasi Proaktif

Untuk langkah-langkah tentang cara menjalankan aturan ini dalam mode proaktif, lihat Mengevaluasi Sumber Daya Anda dengan AWS Config Aturan. Agar aturan ini mengembalikan COMPLIANT dalam mode proaktif, skema konfigurasi sumber daya untuk StartResourceEvaluationAPI harus menyertakan input berikut, yang dikodekan sebagai string:

```
"ResourceConfiguration":
```

```
...
{
   "NodeToNodeEncryptionOptions": BOOLEAN
}
...
```

Untuk informasi lebih lanjut tentang evaluasi proaktif, lihat Mode Evaluasi.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

elastic-beanstalk-logs-to-jam tangan awan

Memeriksa apakah lingkungan AWS Elastic Beanstalk dikonfigurasi untuk mengirim log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika nilai `StreamLogs` salah.

Pengidentifikasi: ELASTIC_BEANSTALK_LOGS_TO_CLOUDWATCH

Jenis Sumber Daya: AWS::ElasticBeanstalk::Environment

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

RetentionInDays (Opsional), Tipe: String

> Memeriksa jumlah hari untuk menyimpan peristiwa log sebelum kedaluwarsa. Nilai yang valid adalah: 1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365, 400, 545, 731, 1827, 3653. Aturannya adalah NON_COMPLIANT jika nilai `logs. RetentionInDays`tidak cocok dengan parameter ini.

DeleteOnTerminate (Opsional), Tipe: String

> Memeriksa apakah log dikonfigurasi untuk dihapus setelah penghentian lingkungan. Nilai yang valid adalah `benar` atau `salah`. Aturannya adalah NON_COMPLIANT jika nilai `logs. DeleteOnTerminate`tidak cocok dengan parameter ini.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

elastic-beanstalk-managed-updates-diaktifkan

Memeriksa apakah pembaruan platform terkelola di AWS Elastic Beanstalk lingkungan diaktifkan. Aturannya adalah COMPLIANT jika nilai untuk `ManagedActionsEnabled` disetel ke true. Aturannya adalah NON_COMPLIANT jika nilai untuk `ManagedActionsEnabled` disetel ke false, atau jika parameter disediakan dan nilainya tidak cocok dengan konfigurasi yang ada.

Pengidentifikasi: ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED

Jenis Sumber Daya: AWS::ElasticBeanstalk::Environment

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Eropa (Zuryol) lich) Wilayah

Parameter:

UpdateLevel (Opsional), Tipe: String

> Menunjukkan apakah tingkat pembaruan disetel ke pembaruan versi 'minor' atau pembaruan versi 'tambalan'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

elbv2- acm-certificate-required

Memeriksa apakah Application Load Balancers dan Network Load Balancer memiliki pendengar yang dikonfigurasi untuk menggunakan sertifikat dari (ACM). AWS Certificate Manager Aturan ini NON_COMPLIANT jika setidaknya 1 penyeimbang beban memiliki setidaknya 1 pendengar yang dikonfigurasi tanpa sertifikat dari ACM atau dikonfigurasi dengan sertifikat yang berbeda dari sertifikat ACM.

Pengidentifikasi: ELBV2 _ACM_CERTIFICATE_REQUIRED

Jenis Sumber Daya: AWS::ElasticLoadBalancingV2::LoadBalancer

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur), AWS GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

AcmCertificatesAllowed (Opsional), Jenis: CSV

Daftar sertifikat Amazon Resource Names () ARNs yang dipisahkan koma.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

elbv2- listener-encryption-in-transit

Memeriksa apakah pendengar untuk penyeimbang beban dikonfigurasi dengan penghentian HTTPS atau TLS. Aturannya adalah NON_COMPLIANT jika pendengar tidak dikonfigurasi dengan penghentian HTTPS atau TLS.

Pengidentifikasi: ELBV2 _LISTENER_ENCRYPTION_IN_TRANSIT

Jenis Sumber Daya: AWS::ElasticLoadBalancingV2::Listener

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Seoul), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Eropa (Zuryol) lich) Wilayah

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

elbv2-multiple-az

Memeriksa apakah Elastic Load Balancer V2 (Application, Network, atau Gateway Load Balancer) dipetakan ke beberapa Availability Zones (). AZs Aturannya adalah NON_COMPLIANT jika Elastic Load Balancer V2 dipetakan menjadi kurang dari 2. AZs Untuk informasi selengkapnya, lihat Availability Zone untuk Application Load Balancer Anda.

Pengidentifikasi: ELBV2 _MULTIPLE_AZ

Jenis Sumber Daya: AWS::ElasticLoadBalancingV2::LoadBalancer

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), AWS GovCloud (AS-Timur), AWS GovCloud (AS-Barat), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

minAvailabilityZones (Opsional), Jenis: int

Jumlah minimum yang diharapkan AZs (antara 2 dan 10 inklusif).

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

elbv2- -periksa predefined-security-policy-ssl

Memeriksa apakah pendengar untuk Application Load Balancers (ALBs) atau Network Load Balancers (NLBs) menggunakan kebijakan keamanan tertentu. Aturannya adalah NON_COMPLIANT jika pendengar HTTPS untuk ALB atau pendengar TLS untuk NLB tidak menggunakan kebijakan keamanan yang Anda tentukan.

Pengidentifikasi: _PREDEFINED_SECURITY_POLICY_SSL_CHECK ELBV2

Jenis Sumber Daya: AWS::ElasticLoadBalancingV2::Listener

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (Bahrain), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok Wilayah (Ningxia), Eropa (Zurich)

Parameter:

Kebijakan SSL, Jenis: CSV

> Daftar kebijakan keamanan SSL yang dipisahkan koma untuk diperiksa aturan. Misalnya, "ELBSecurityKebijakan- TLS13 -1-2-2021-06".

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

elb-acm-certificate-required

Memeriksa apakah Classic Load Balancer menggunakan sertifikat SSL yang disediakan oleh. AWS Certificate Manager Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.

Pengidentifikasi: ELB_ACM_CERTIFICATE_REQUIRED

Jenis Sumber Daya: AWS::ElasticLoadBalancing::LoadBalancer

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Afrika (Cape Town), Asia Pasifik (Osaka), Eropa (Milan), Israel (Tel Aviv), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

elb-cross-zone-load-menyeimbangkan diaktifkan

Memeriksa apakah penyeimbangan beban lintas zona diaktifkan untuk Classic Load Balancer. Aturannya adalah NON_COMPLIANT jika penyeimbangan beban lintas zona tidak diaktifkan untuk Classic Load Balancers.

Pengidentifikasi: ELB_CROSS_ZONE_LOAD_BALANCING_ENABLED

Jenis Sumber Daya: AWS::ElasticLoadBalancing::LoadBalancer

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

elb-custom-security-policy-ssl-periksa

Memeriksa apakah pendengar Classic Load Balancer SSL Anda menggunakan kebijakan khusus. Aturan ini hanya berlaku jika ada pendengar SSL untuk Classic Load Balancer.

Pengidentifikasi: ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK

Jenis Sumber Daya: AWS::ElasticLoadBalancing::LoadBalancer

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Jakarta), Asia Pasifik (Osaka), Asia Pasifik (Melbourne), Wilayah Asia Pasifik (Taipei)

Parameter:

sslProtocolsAndCipher, Tipe: String

Daftar cipher dan protokol dipisahkan koma.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

elb-deletion-protection-enabled

Memeriksa apakah Elastic Load Balancer mengaktifkan proteksi penghapusan. Aturannya adalah NON_COMPLIANT jika deletion_protection.enabled salah.

Pengidentifikasi: ELB_DELETION_PROTECTION_ENABLED

Jenis Sumber Daya: AWS::ElasticLoadBalancingV2::LoadBalancer

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Osaka)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

elb-logging-enabled

Memeriksa apakah Application Load Balancer dan Classic Load Balancer telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika false atau `access_logs.S3.bucket` tidak sama dengan s3 BucketName yang Anda berikan. `access_logs.s3.enabled`

> **Note**
>
> Aturan ini tidak berlaku untuk Network Load Balancers atau Gateway Load Balancers.

Pengidentifikasi: ELB_LOGGING_ENABLED

Jenis Sumber Daya: AWS::ElasticLoadBalancing::LoadBalancer, AWS::ElasticLoadBalancingV2::LoadBalancer

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

s3 BucketNames (Opsional), Jenis: CSV

Daftar nama bucket Amazon S3 yang dipisahkan koma untuk Amazon ELB untuk mengirimkan file log.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

elb-predefined-security-policy-ssl-periksa

Memeriksa apakah pendengar SSL Classic Load Balancer Anda menggunakan kebijakan yang telah ditentukan sebelumnya. Aturannya adalah NON_COMPLIANT jika kebijakan pendengar Classic Load HTTPS/SSL Balancer tidak sama dengan nilai parameter ". `predefinedPolicyName`

Pengidentifikasi: ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK

Jenis Sumber Daya: AWS::ElasticLoadBalancing::LoadBalancer

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Osaka)

Parameter:

predefinedPolicyName, Tipe: String

Nama kebijakan yang telah ditentukan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

elb-tls-https-listeners-hanya

Memeriksa apakah Classic Load Balancer Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Aturannya adalah NON_COMPLIANT jika pendengar tidak dikonfigurasi dengan SSL atau HTTPS.

- Jika Classic Load Balancer tidak memiliki listener yang dikonfigurasi, maka aturan akan kembali. `NOT_APPLICABLE`
- Aturannya SESUAI jika pendengar Classic Load Balancer dikonfigurasi dengan SSL atau HTTPS.
- Aturannya adalah NON_COMPLIANT jika pendengar tidak dikonfigurasi dengan SSL atau HTTPS.

Pengidentifikasi: ELB_TLS_HTTPS_LISTENERS_ONLY

Jenis Sumber Daya: AWS::ElasticLoadBalancing::LoadBalancer

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Timur Tengah (UEA), Asia Pasifik (Osaka)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

emr-block-public-access

Memeriksa apakah akun dengan Amazon EMR telah mengaktifkan pengaturan akses publik yang memblokir. Aturannya adalah NON_COMPLIANT jika BlockPublicSecurityGroupRules salah, atau jika benar, port selain Port 22 terdaftar di. PermittedPublicSecurityGroupRuleRanges

Pengidentifikasi: EMR_BLOCK_PUBLIC_ACCESS

Jenis Sumber Daya: AWS: :::Akun

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Tiongkok (Ningxia) Wilayah

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

emr-kerberos-enabled

Memeriksa apakah cluster EMR Amazon mengaktifkan Kerberos. Aturannya adalah NON_COMPLIANT jika konfigurasi keamanan tidak dilampirkan ke cluster atau konfigurasi keamanan tidak memenuhi parameter aturan yang ditentukan.

Pengidentifikasi: EMR_KERBEROS_ENABLED

Jenis Sumber Daya: AWS::EMR::Cluster

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei), Kanada Barat (Calgary)

Parameter:

TicketLifetimeInHours (Opsional), Jenis: int

Periode dimana tiket Kerberos yang dikeluarkan oleh KDC klaster berlaku.

Realm (Opsional), Tipe: String

Nama ranah Kereberos dari ranah lain dalam hubungan kepercayaan.

Domain (Opsional), Tipe: String

Nama domain dari ranah lain dalam hubungan kepercayaan.

AdminServer (Opsional), Tipe: String

Domain yang sepenuhnya memenuhi syarat dari server admin di ranah lain dari hubungan kepercayaan.

KdcServer (Opsional), Tipe: String

Domain yang sepenuhnya memenuhi syarat dari server KDC di ranah lain dari hubungan kepercayaan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

emr-master-no-public-ip

Memeriksa apakah node master cluster EMR Amazon memiliki publik. IPs Aturannya adalah NON_COMPLIANT jika node master memiliki IP publik.

> **Note**
>
> Aturan ini memeriksa cluster yang berada dalam status RUNNING atau WAITING. Aturan ini mengharuskan Anda untuk mengaktifkan perekaman untuk jenis `AWS::EC2::Instance` sumber daya agar memiliki evaluasi yang akurat.

Pengidentifikasi: EMR_MASTER_NO_PUBLIC_IP

Jenis Sumber Daya: AWS::EMR::Cluster, AWS::EC2::Instance

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Osaka), Asia Pasifik (Melbourne), Israel (Tel Aviv), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

emr-security-configuration-encryption-istirahat

Memeriksa apakah konfigurasi keamanan EMR Amazon mengaktifkan enkripsi saat istirahat. Aturannya adalah NON_COMPLIANT jika konfigurasi. SecurityConfiguration. EncryptionConfiguration. EnableAtRestEncryption adalah palsu.

Pengidentifikasi: EMR_SECURITY_CONFIGURATION_ENCRYPTION_REST

Jenis Sumber Daya: AWS::EMR::SecurityConfiguration

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

emr-security-configuration-encryption-transit

Memeriksa apakah konfigurasi keamanan EMR Amazon mengaktifkan enkripsi saat transit. Aturannya adalah NON_COMPLIANT jika konfigurasi. SecurityConfiguration. EncryptionConfiguration. EnableInTransitEncryption adalah palsu.

Pengidentifikasi: EMR_SECURITY_CONFIGURATION_ENCRYPTION_TRANSIT

Jenis Sumber Daya: AWS::EMR::SecurityConfiguration

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

volume terenkripsi

Memeriksa apakah volume Amazon EBS terlampir dienkripsi dan secara opsional dienkripsi dengan kunci KMS tertentu. Aturannya adalah NON_COMPLIANT jika volume EBS terlampir tidak dienkripsi atau dienkripsi dengan kunci KMS yang tidak ada dalam parameter yang disediakan.

Pengidentifikasi: ENCRYPTED_VOLUME

Jenis Sumber Daya: AWS::EC2::Volume

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

KMSid (Opsional), Tipe: String

ID atau ARN dari kunci KMS yang digunakan untuk mengenkripsi volume.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

event-data-store-cmk-enkripsi diaktifkan

Memeriksa apakah AWS penyimpanan data peristiwa Cloud Trail mengaktifkan kunci AWS KMS yang dikelola pelanggan. Aturannya adalah NON_COMPLIANT jika penyimpanan data peristiwa telah menonaktifkan kunci KMS yang dikelola pelanggan. Secara opsional, Anda dapat menentukan daftar kunci KMS untuk diperiksa aturan.

Pengidentifikasi: EVENT_DATA_STORE_CMK_ENCRYPTION_ENABLED

Jenis Sumber Daya: AWS::CloudTrail::EventDataStore

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (Bahrain), Tiongkok (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

kmsKeyArns (Opsional), Jenis: CSV

> Daftar Amazon Resource Names (ARNs) kunci AWS KMS yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika penyimpanan data peristiwa AWS Cloud Trail tidak dienkripsi dengan salah satu kunci KMS ini.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

evidently-launch-description

Memeriksa apakah Amazon CloudWatch Jelas diluncurkan memiliki deskripsi. Aturannya adalah NON_COMPLIANT jika Configuration.description tidak ada atau string kosong.

Pengidentifikasi: EVIDENTLY_LAUNCH_DESCRIPTION

Jenis Sumber Daya: AWS::Evidently::Launch

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Eropa (Stockholm), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney) Wilayah

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

evidently-launch-tagged

Memeriksa apakah Amazon CloudWatch Jelas meluncurkan tag memiliki. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: EVIDENTLY_LAUNCH_TAGGED

Jenis Sumber Daya: AWS::Evidently::Launch

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Eropa (Stockholm), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney) Wilayah

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

evidently-project-description

Memeriksa apakah Amazon CloudWatch Terbukti proyek memiliki deskripsi. Aturannya adalah NON_COMPLIANT jika Configuration.description tidak ada atau string kosong.

Pengidentifikasi: EVIDENTLY_PROJECT_DESCRIPTION

Jenis Sumber Daya: AWS::Evidently::Project

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Eropa (Stockholm), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney) Wilayah

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

evidently-project-tagged

Memeriksa apakah Amazon CloudWatch Ternyata proyek memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: EVIDENTLY_PROJECT_TAGGED

Jenis Sumber Daya: AWS::Evidently::Project

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Eropa (Stockholm), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney) Wilayah

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

evidently-segment-description

Memeriksa apakah Amazon CloudWatch Terbukti segmen memiliki deskripsi. Aturannya adalah NON_COMPLIANT jika Configuration.description tidak ada atau string kosong.

Pengidentifikasi: EVIDENTLY_SEGMENT_DESCRIPTION

Jenis Sumber Daya: AWS::Evidently::Segment

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Eropa (Stockholm), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney) Wilayah

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

evidently-segment-tagged

Memeriksa apakah Amazon CloudWatch Terbukti segmen memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: EVIDENTLY_SEGMENT_TAGGED

Jenis Sumber Daya: AWS::Evidently::Segment

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Eropa (Stockholm), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney) Wilayah

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

fis-experiment-template-log-konfigurasi-ada

Memeriksa apakah templat eksperimen AWS FIS memiliki pencatatan eksperimen yang dikonfigurasi. Aturannya adalah NON_COMPLIANT jika konfigurasi. LogConfiguration tidak ada.

Pengidentifikasi: FIS_EXPERIMENT_TEMPLATE_LOG_CONFIGURATION_EXISTS

Jenis Sumber Daya: AWS::FIS::ExperimentTemplate

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat), Meksiko (Tengah) AWS GovCloud , Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

fis-experiment-template-tagged

Memeriksa apakah templat eksperimen AWS FIS memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: FIS_EXPERIMENT_TEMPLATE_TAGGED

Jenis Sumber Daya: AWS::FIS::ExperimentTemplate

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat), Meksiko (Tengah) AWS GovCloud , Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

fms-shield-resource-policy-periksa

Memeriksa apakah sumber daya yang dapat dilindungi oleh AWS Shield Advanced dilindungi oleh Shield Advanced. Aturannya adalah NON_COMPLIANT jika sumber daya tertentu tidak dilindungi.

Pengidentifikasi: FMS_SHIELD_RESOURCE_POLICY_CHECK

Jenis Sumber Daya: AWS::CloudFront::Distribution, AWS::ElasticLoadBalancingV2::LoadBalancer, AWS::WAFRegional::WebACL, AWS::EC2::EIP, AWS::ElasticLoadBalancing::LoadBalancer, AWS::ShieldRegional::Protection, AWS::Shield::Protection

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

web ACLId, Tipe: String

Pengenal unik untuk Web ACL.

resourceTypes, Tipe: String

Jenis sumber daya yang Anda tentukan untuk diperiksa aturan.

ResourceTags (Opsional), Tipe: String

Tag sumber daya yang Anda tentukan untuk diperiksa aturan. Misalnya, {“tagKey1": [" tagValue1"], “tagKey2": [" tagValue2", “tagValue3"]}.

excludeResourceTags (Opsional), Jenis: boolean

Jika benar, aturan mengecualikan sumber daya yang ditentukan dalam ResourceTags. Jika salah, aturan mencakup semua sumber daya yang ditentukan dalam ResourceTags.

fmsManagedToken (Opsional), Tipe: String

Token yang dihasilkan oleh AWS Firewall Manager saat membuat aturan di akun Anda. AWS Config mengabaikan parameter ini saat Anda membuat aturan ini.

fmsRemediationEnabled (Opsional), Jenis: boolean

Jika benar, AWS Firewall Manager akan memperbarui sumber daya NON_COMPLIANT sesuai dengan kebijakan FMS. AWS Config mengabaikan parameter ini saat Anda membuat aturan ini.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

fms-webacl-resource-policy-periksa

Memeriksa apakah ACL web dikaitkan dengan Application Load Balancer, tahap API Gateway, atau distribusi Amazon CloudFront . Saat AWS Firewall Manager membuat aturan ini, pemilik kebijakan FMS menentukan kebijakan FMS dan `WebACLId` secara opsional dapat mengaktifkan remediasi.

Pengidentifikasi: FMS_WEBACL_RESOURCE_POLICY_CHECK

Jenis Sumber Daya: AWS::CloudFront::Distribution, AWS::ApiGateway::Stage, AWS::ElasticLoadBalancingV2::LoadBalancer, AWS::WAFRegional::WebACL

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

web ACLId, Tipe: String

Web ACLId dari web ACL.

ResourceTags (Opsional), Tipe: String

Tag sumber daya (ApplicationLoadBalancer, ApiGatewayStage dan CloudFront distribusi) yang harus dikaitkan dengan aturan. (misalnya, {“tagKey1": [" tagValue1"], “tagKey2": [" tagValue2", “tagValue3"]})

excludeResourceTags (Opsional), Jenis: boolean

Jika benar, kecualikan sumber daya yang cocok dengan ResourceTags.

fmsManagedToken (Opsional), Tipe: String

Token yang dihasilkan oleh AWS Firewall Manager saat membuat aturan di akun pelanggan. AWS Config mengabaikan parameter ini saat pelanggan membuat aturan ini.

fmsRemediationEnabled (Opsional), Jenis: boolean

Jika benar, AWS Firewall Manager akan memperbarui sumber daya yang tidak sesuai sesuai dengan kebijakan FMS. AWS Config mengabaikan parameter ini saat pelanggan membuat aturan ini.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

fms-webacl-rulegroup-association-periksa

Memeriksa apakah grup aturan terkait dengan ACL web pada prioritas yang benar. Prioritas yang benar ditentukan oleh peringkat kelompok aturan dalam parameter RuleGroups. Ketika AWS Firewall Manager membuat aturan ini, ia menetapkan prioritas tertinggi 0 diikuti oleh 1, 2, dan seterusnya. Pemilik kebijakan FMS menentukan `ruleGroups` peringkat dalam kebijakan FMS dan secara opsional dapat mengaktifkan remediasi.

Pengidentifikasi: FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK

Jenis Sumber Daya: AWS::WAF::WebACL, AWS::WAFRegional::WebACL

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

ruleGroups, Tipe: String

Daftar dan pasangan yang dipisahkan koma. RuleGroupIds WafOverrideAction (misalnya, ruleGroupId -1:NONE, ruleGroupId 2:COUNT)

fmsManagedToken (Opsional), Tipe: String

Token yang dihasilkan oleh AWS Firewall Manager saat membuat aturan di akun pelanggan. AWS Config mengabaikan parameter ini saat pelanggan membuat aturan ini.

fmsRemediationEnabled (Opsional), Jenis: boolean

Jika benar, AWS Firewall Manager akan memperbarui sumber daya yang tidak sesuai sesuai dengan kebijakan FMS. AWS Config mengabaikan parameter ini saat pelanggan membuat aturan ini.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

frauddetector-entity-type-tagged

Memeriksa apakah jenis entitas Amazon Fraud Detector memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk aturan tersebut. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: FRAUDDETECTOR_ENTITY_TYPE_TAGGED

Jenis Sumber Daya: AWS::FraudDetector::EntityType

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di AS Timur (Ohio), Eropa (Irlandia), AS Timur (Virginia N.), AS Barat (Oregon), Asia Pasifik (Singapura), Wilayah Asia Pasifik (Sydney)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

frauddetector-label-tagged

Memeriksa apakah label Amazon Fraud Detector memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk aturan tersebut. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: FRAUDDETECTOR_LABEL_TAGGED

Jenis Sumber Daya: AWS::FraudDetector::Label

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di AS Timur (Ohio), Eropa (Irlandia), AS Timur (Virginia N.), AS Barat (Oregon), Asia Pasifik (Singapura), Wilayah Asia Pasifik (Sydney)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

frauddetector-outcome-tagged

Memeriksa apakah hasil Amazon Fraud Detector memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk aturan tersebut. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: FRAUDDETECTOR_OUTCOME_TAGGED

Jenis Sumber Daya: AWS::FraudDetector::Outcome

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di AS Timur (Ohio), Eropa (Irlandia), AS Timur (Virginia N.), AS Barat (Oregon), Asia Pasifik (Singapura), Wilayah Asia Pasifik (Sydney)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

frauddetector-variable-tagged

Memeriksa apakah variabel Amazon Fraud Detector memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk aturan tersebut. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: FRAUDDETECTOR_VARIABLE_TAGGED

Jenis Sumber Daya: AWS::FraudDetector::Variable

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di AS Timur (Ohio), Eropa (Irlandia), AS Timur (Virginia N.), AS Barat (Oregon), Asia Pasifik (Singapura), Wilayah Asia Pasifik (Sydney)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

fsx-last-backup-recovery-point-dibuat

Memeriksa apakah titik pemulihan dibuat untuk Amazon FSx File Systems. Aturannya adalah NON_COMPLIANT jika Sistem FSx File Amazon tidak memiliki titik pemulihan yang sesuai yang dibuat dalam periode waktu yang ditentukan.

Pengidentifikasi: FSX_LAST_BACKUP_RECOVERY_POINT_CREATED

Jenis Sumber Daya: AWS::FSx::FileSystem

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

ResourceTags (Opsional), Tipe: String

Tag Sistem FSx File Amazon untuk aturan yang akan diperiksa, dalam format `{"tagkey" : "tagValue"}` JSON.

ResourceID (Opsional), Tipe: String

ID Sistem FSx File Amazon untuk aturan yang akan diperiksa.

recoveryPointAgeNilai (Opsional), Jenis: int, Default: 1

Nilai numerik untuk usia maksimum yang diizinkan. Tidak lebih dari 744 jam, 31 untuk hari.

recoveryPointAgeUnit (Opsional), Tipe: String, Default: hari

Satuan waktu untuk usia maksimum yang diizinkan. Nilai yang diterima: 'jam', 'hari'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

fsx-lustre-copy-tagsuntuk cadangan

Memeriksa apakah sistem file Amazon FSx untuk Lustre dikonfigurasi untuk menyalin tag ke cadangan. Aturannya adalah NON_COMPLIANT jika sistem file Lustre tidak dikonfigurasi untuk menyalin tag ke cadangan.

Pengidentifikasi: FSX_LUSTRE_COPY_TAGS_TO_BACKUPS

Jenis Sumber Daya: AWS::FSx::FileSystem

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Tiongkok (Ningxia) Wilayah

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

fsx-meets-restore-time-target

Memeriksa apakah waktu pemulihan Sistem FSx File Amazon memenuhi durasi yang ditentukan. Aturannya adalah NON_COMPLIANT jika LatestRestoreExecutionTimeMinutes Sistem FSx File Amazon lebih besar dari menit. maxRestoreTime

Pengidentifikasi: FSX_MEETS_RESTORE_TIME_TARGET

Jenis Sumber Daya: AWS::FSx::FileSystem

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

maxRestoreTime, Jenis: int

Nilai numerik untuk runtime pemulihan maksimum yang diizinkan.

ResourceTags (Opsional), Tipe: String

Tag Sistem FSx File Amazon untuk aturan yang akan diperiksa, dalam format JSON.

ResourceID (Opsional), Tipe: String

ID Sistem FSx File Amazon untuk aturan yang akan diperiksa.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

fsx-ontap-deployment-type-periksa

Memeriksa apakah Amazon FSx untuk sistem file NetApp ONTAP dikonfigurasi dengan jenis penerapan tertentu. Aturannya adalah NON_COMPLIANT jika sistem file Amazon FSx untuk NetApp ONTAP tidak dikonfigurasi dengan jenis penerapan yang Anda tentukan.

Pengidentifikasi: FSX_ONTAP_DEPLOYMENT_TYPE_CHECK

Jenis Sumber Daya: AWS::FSx::FileSystem

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (Bahrain), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

DeploymentTypes, Jenis: CSV

Daftar tipe Deployment yang diizinkan dipisahkan koma untuk diperiksa oleh aturan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

fsx-openzfs-copy-tags-diaktifkan

Memeriksa apakah sistem file Amazon FSx untuk OpenZFS dikonfigurasi untuk menyalin tag ke cadangan dan volume. Aturannya adalah NON_COMPLIANT jika FSx untuk sistem file OpenZFS tidak dikonfigurasi untuk menyalin tag ke backup dan volume.

Pengidentifikasi: FSX_OPENZFS_COPY_TAGS_ENABLED

Jenis Sumber Daya: AWS::FSx::FileSystem

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

fsx-openzfs-deployment-type-periksa

Memeriksa apakah sistem file Amazon FSx untuk OpenZFS dikonfigurasi dengan jenis penyebaran tertentu. Aturannya adalah NON_COMPLIANT jika FSx untuk sistem file OpenZFS tidak dikonfigurasi dengan jenis penerapan yang Anda tentukan.

Pengidentifikasi: FSX_OPENZFS_DEPLOYMENT_TYPE_CHECK

Jenis Sumber Daya: AWS::FSx::FileSystem

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (Bahrain), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

DeploymentTypes, Jenis: CSV

Daftar tipe Deployment yang diizinkan dipisahkan koma untuk diperiksa oleh aturan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

fsx-resources-protected-by-rencana cadangan

Memeriksa apakah Sistem FSx File Amazon dilindungi oleh paket cadangan. Aturannya adalah NON_COMPLIANT jika Sistem FSx File Amazon tidak dicakup oleh paket cadangan.

Pengidentifikasi: FSX_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Jenis Sumber Daya: AWS::FSx::FileSystem

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

ResourceTags (Opsional), Tipe: String

Tag Sistem FSx File Amazon untuk aturan yang akan diperiksa, dalam format `{"tagkey" : "tagValue"}` JSON.

ResourceID (Opsional), Tipe: String

ID Sistem FSx File Amazon untuk aturan yang akan diperiksa.

crossRegionList (Opsional), Tipe: String

Daftar wilayah tujuan yang dipisahkan koma untuk salinan cadangan lintas wilayah yang akan disimpan

crossAccountList (Opsional), Tipe: String

Daftar akun tujuan yang dipisahkan koma untuk salinan cadangan lintas akun yang akan disimpan

maxRetentionDays (Opsional), Jenis: int

Periode retensi maksimum dalam beberapa hari untuk Backup Vault Lock

minRetentionDays (Opsional), Jenis: int

Periode retensi minimum dalam beberapa hari untuk Backup Vault Lock

backupVaultLockPeriksa (Opsional), Tipe: String

Nilai yang diterima: 'Benar' atau 'False'. Masukkan 'Benar' untuk aturan untuk memeriksa apakah sumber daya dicadangkan di brankas yang terkunci

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

fsx-windows-audit-log-dikonfigurasi

Memeriksa apakah sistem file Amazon FSx untuk Windows File Server mengaktifkan audit akses file. Aturannya adalah NON_COMPLIANT jika FSx untuk sistem file Windows File Server tidak mengaktifkan audit akses file.

Pengidentifikasi: FSX_WINDOWS_AUDIT_LOG_CONFIGURATED

Jenis Sumber Daya: AWS::FSx::FileSystem

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

fsx-windows-deployment-type-periksa

Memeriksa apakah sistem file Amazon FSx untuk WINDOWS dikonfigurasi dengan jenis penyebaran tertentu. Aturannya adalah NON_COMPLIANT jika FSx untuk sistem file WINDOWS tidak dikonfigurasi dengan jenis penerapan yang Anda tentukan.

Pengidentifikasi: FSX_WINDOWS_DEPLOYMENT_TYPE_CHECK

Jenis Sumber Daya: AWS::FSx::FileSystem

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (Bahrain), Tiongkok (Beijing), Asia Pasifik (Thailand), Eropa (Paris), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

DeploymentTypes, Jenis: CSV

Daftar tipe Deployment yang diizinkan dipisahkan koma untuk diperiksa oleh aturan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

glb-listener-tagged

Memeriksa apakah pendengar Load Balancer Gateway memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: GLB_LISTENER_TAGGED

Jenis Sumber Daya: AWS::ElasticLoadBalancingV2::Listener

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

global-endpoint-event-replication-diaktifkan

Memeriksa apakah replikasi peristiwa diaktifkan untuk titik akhir EventBridge global Amazon. Aturannya adalah NON_COMPLIANT jika replikasi acara tidak diaktifkan.

Pengidentifikasi: GLOBAL_ENDPOINT_EVENT_REPLICATION_ENABLED

Jenis Sumber Daya: AWS::Events::Endpoint

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Eropa (Stockholm), Asia Pasifik (Mumbai), Eropa (Paris), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), Amerika Selatan (Sao Paulo), AS Timur (Virginia N), Asia Pasifik (Seoul), Asia Pasifik (Osaka), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), AS Barat (N. California), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Wilayah Kanada (Tengah)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

glue-job-logging-enabled

Memeriksa apakah pekerjaan AWS Glue telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika pekerjaan AWS Glue tidak mengaktifkan log Amazon CloudWatch .

Pengidentifikasi: GLUE_JOB_LOGGING_ENABLED

Jenis Sumber Daya: AWS::Glue::Job

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

glue-ml-transform-encrypted-saat istirahat

Memeriksa apakah AWS Glue MLTransform memiliki enkripsi saat istirahat diaktifkan. Aturannya adalah NON_COMPLIANT jika `diatur ke MLUser DataEncryptionMode `DISABLED`.

Pengidentifikasi: GLUE_ML_TRANSFORM_ENCRYPTED_AT_REST

Jenis Sumber Daya: AWS::Glue::MLTransform

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), AWS GovCloud (AS-Timur), Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

glue-spark-job-supported-versi

Memeriksa apakah pekerjaan AWS Glue Spark berjalan pada versi AWS Glue minimum yang didukung. Aturannya adalah NON_COMPLIANT jika pekerjaan AWS Glue Spark tidak berjalan pada versi AWS Glue minimum yang didukung yang Anda tentukan.

Pengidentifikasi: GLUE_SPARK_JOB_SUPPORTED_VERSION

Jenis Sumber Daya: AWS::Glue::Job

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (Bahrain), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

minimumSupportedGlueVersi, Tipe: String

> Nilai string Anda harus menentukan versi AWS Glue minimum yang didukung agar aturan diperiksa.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

penjaga-ec2- protection-runtime-enabled

Memeriksa apakah ECS Runtime Monitoring dengan manajemen agen otomatis diaktifkan untuk detektor Amazon GuardDuty . Aturannya adalah NON_COMPLIANT jika fitur tersebut tidak diaktifkan untuk akun Anda atau setidaknya satu akun anggota di organisasi Anda.

Pengidentifikasi: EC2 GUARDDUTY_ _PROTECTION_RUNTIME_ENABLED

Jenis Sumber Daya: AWS::GuardDuty::Detector

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (Bahrain), Tiongkok (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur), AWS GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

guardduty-ecs-protection-runtime-diaktifkan

Memeriksa apakah ECS Runtime Monitoring dengan manajemen agen otomatis diaktifkan untuk detektor Amazon GuardDuty . Aturannya adalah NON_COMPLIANT jika fitur tersebut tidak diaktifkan untuk akun Anda atau setidaknya satu akun anggota di organisasi Anda.

Pengidentifikasi: GUARDDUTY_ECS_PROTECTION_RUNTIME_ENABLED

Jenis Sumber Daya: AWS::GuardDuty::Detector

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (Bahrain), Tiongkok (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur), AWS GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

guardduty-eks-protection-audit-diaktifkan

Memeriksa apakah Pemantauan Log Audit untuk Amazon Elastic Kubernetes Service (Amazon EKS) diaktifkan untuk detektor GuardDuty Amazon di akun Anda. Aturannya adalah NON_COMPLIANT jika fitur Pemantauan Log Audit EKS tidak diaktifkan untuk akun Anda.

Pengidentifikasi: GUARDDUTY_EKS_PROTECTION_AUDIT_ENABLED

Jenis Sumber Daya: AWS::GuardDuty::Detector

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

guardduty-eks-protection-runtime-diaktifkan

Memeriksa apakah Amazon EKS Runtime Monitoring dengan manajemen agen otomatis diaktifkan untuk GuardDuty detektor di akun Anda. Aturannya adalah NON_COMPLIANT jika EKS Runtime Monitoring dengan manajemen agen otomatis di tidak GuardDuty diaktifkan untuk akun Anda.

Pengidentifikasi: GUARDDUTY_EKS_PROTECTION_RUNTIME_ENABLED

Jenis Sumber Daya: AWS::GuardDuty::Detector

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Tiongkok (Ningxia) Wilayah

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

guardduty-enabled-centralized

Memeriksa GuardDuty apakah Amazon diaktifkan di AWS akun dan AWS Wilayah Anda. Jika Anda memberikan AWS akun untuk sentralisasi, aturan mengevaluasi GuardDuty hasil dalam akun terpusat. Aturannya adalah COMPLIANT saat GuardDuty diaktifkan.

Pengidentifikasi: GUARDDUTY_ENABLED_CENTRALIZED

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Meksiko (Tengah), Wilayah Asia Pasifik (Taipei)

Parameter:

CentralMonitoringAccount (Opsional), Tipe: String

> Daftar AWS Akun yang dipisahkan koma (12 digit) di mana GuardDuty hasil Amazon diizinkan untuk dipusatkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

guardduty-lambda-protection-enabled

Memeriksa apakah Perlindungan Lambda diaktifkan untuk GuardDuty detektor Amazon di akun Anda. Aturannya adalah NON_COMPLIANT jika fitur Perlindungan Lambda di Amazon tidak GuardDuty diaktifkan untuk akun Anda.

Pengidentifikasi: GUARDDUTY_LAMBDA_PROTECTION_ENABLED

Jenis Sumber Daya: AWS::GuardDuty::Detector

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

guardduty-malware-protection-enabled

Memeriksa apakah Perlindungan Malware diaktifkan untuk GuardDuty detektor Amazon di akun Anda. Aturannya adalah NON_COMPLIANT jika fitur Perlindungan Malware di Amazon tidak GuardDuty diaktifkan untuk akun Anda.

Pengidentifikasi: GUARDDUTY_MALWARE_PROTECTION_ENABLED

Jenis Sumber Daya: AWS::GuardDuty::Detector

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Tiongkok (Ningxia) Wilayah

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

guardduty-non-archived-findings

Memeriksa apakah Amazon GuardDuty memiliki temuan yang tidak diarsipkan. Aturannya adalah NON_COMPLIANT jika GuardDuty memiliki parameter/yang tidak low/medium/high severity findings older than the specified number in the daysLowSev/daysMediumSev diarsipkan. `daysHighSev`

Pengidentifikasi: GUARDDUTY_NON_ARCHIVED_TEMUAN-TEMUAN

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Meksiko (Tengah), Wilayah Asia Pasifik (Taipei)

Parameter:

daysLowSev (Opsional), Jenis: int, Bawaan: 30

Jumlah hari temuan tingkat keparahan GuardDuty rendah Amazon diizinkan untuk tetap tidak diarsipkan. Defaultnya adalah 30 hari.

daysMediumSev (Opsional), Jenis: int, Default: 7

Jumlah hari temuan tingkat keparahan GuardDuty menengah Amazon diizinkan untuk tetap tidak diarsipkan. Defaultnya adalah 7 hari.

daysHighSev (Opsional), Jenis: int, Default: 1

Jumlah hari temuan tingkat keparahan GuardDuty tinggi Amazon diizinkan untuk tetap tidak diarsipkan. Defaultnya adalah 1 hari.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

guardduty-rds-protection-enabled

Memeriksa apakah perlindungan Amazon Relational Database Service (Amazon RDS) diaktifkan untuk detektor GuardDuty Amazon di akun Anda. Aturannya adalah NON_COMPLIANT jika fitur perlindungan Amazon RDS di Amazon tidak GuardDuty diaktifkan untuk akun Anda.

Pengidentifikasi: GUARDDUTY_RDS_PROTECTION_ENABLED

Jenis Sumber Daya: AWS::GuardDuty::Detector

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Tiongkok (Ningxia) Wilayah

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

guardduty-runtime-monitoring-enabled

Memeriksa apakah Runtime Monitoring diaktifkan untuk GuardDuty detektor Amazon di akun atau organisasi Anda. Aturannya adalah NON_COMPLIANT jika Runtime Monitoring in tidak GuardDuty diaktifkan untuk akun Anda atau setidaknya satu akun anggota di organisasi Anda.

Pengidentifikasi: GUARDDUTY_RUNTIME_MONITORING_ENABLED

Jenis Sumber Daya: AWS::GuardDuty::Detector

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (Bahrain), Tiongkok (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur), AWS GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

guardduty-s3-protection-enabled

Memeriksa apakah Perlindungan S3 diaktifkan untuk GuardDuty Detektor Amazon di akun Anda. Aturannya adalah NON_COMPLIANT jika fitur Perlindungan S3 di Amazon tidak GuardDuty diaktifkan untuk akun Anda.

Pengidentifikasi: GUARDDUTY_S3_PROTECTION_ENABLED

Jenis Sumber Daya: AWS::GuardDuty::Detector

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

iam-customer-policy-blocked-kms-tindakan

Memeriksa apakah kebijakan AWS Identity and Access Management (IAM) terkelola yang Anda buat tidak mengizinkan tindakan KMS yang diblokir pada semua sumber daya kunci KMS. AWS Aturannya adalah NON_COMPLIANT jika ada tindakan yang diblokir diizinkan pada semua kunci AWS KMS oleh kebijakan IAM terkelola.

> **Note**
>
> Agar dianggap non-publik, kebijakan IAM harus memberikan akses hanya ke nilai tetap. Ini berarti nilai yang tidak mengandung wildcard atau elemen kebijakan IAM berikut: Variabel.

Pengidentifikasi: IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS

Jenis Sumber Daya: AWS::IAM::Policy

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

blockedActionsPatterns, Jenis: CSV

Daftar pola tindakan KMS yang diblokir yang dipisahkan koma untuk diperiksa aturan. Aturannya adalah NON_COMPLIANT jika kebijakan yang dikelola pelanggan IAM mengizinkan akses wildcard ke semua sumber daya untuk tindakan yang Anda tentukan.

excludePermissionBoundaryKebijakan (Opsional), Jenis: boolean

Boolean flag untuk mengecualikan evaluasi kebijakan IAM yang digunakan sebagai batas izin. Jika disetel ke 'true', aturan tidak akan menyertakan batas izin dalam evaluasi. Jika tidak, semua kebijakan IAM dalam lingkup dievaluasi ketika nilai disetel ke 'false.' Nilai default adalah 'salah'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

iam-external-access-analyzer-diaktifkan

Memeriksa apakah IAM Access Analyzer untuk akses eksternal diaktifkan di akun Anda per wilayah. Aturannya adalah NON_COMPLIANT jika tidak ada penganalisis untuk akses eksternal di wilayah atau jika atribut 'status' tidak disetel ke 'AKTIF'.

Pengidentifikasi: IAM_EXTERNAL_ACCESS_ANALYZER_ENABLED

Jenis Sumber Daya: AWS: :::Akun

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

iam-group-has-users-periksa

Memeriksa apakah grup IAM memiliki setidaknya satu pengguna IAM.

Pengidentifikasi: IAM_GROUP_HAS_USERS_CHECK

Jenis Sumber Daya: AWS::IAM::Group

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

iam-inline-policy-blocked-kms-tindakan

Memeriksa apakah kebijakan sebaris yang dilampirkan pada pengguna, peran, dan grup IAM Anda tidak mengizinkan tindakan yang diblokir pada semua kunci AWS KMS. Aturannya adalah NON_COMPLIANT jika ada tindakan yang diblokir diizinkan pada semua kunci AWS KMS dalam kebijakan sebaris.

Pengidentifikasi: IAM_INLINE_POLICY_BLOCKED_KMS_ACTIONS

Jenis Sumber Daya: AWS::IAM::Group, AWS::IAM::Role, AWS::IAM::User

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

blockedActionsPatterns, Jenis: CSV

Daftar pola tindakan KMS yang diblokir dengan koma, misalnya, *, kms: Dekripsi, kms: *. kms: ReEncrypt

excludeRoleByManagementAccount (Opsional), Jenis: boolean

Kecualikan peran jika hanya dapat diasumsikan oleh akun manajemen organisasi.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

iam-no-inline-policy-periksa

Memeriksa apakah fitur kebijakan inline tidak digunakan. Aturannya adalah NON_COMPLIANT jika pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM memiliki kebijakan sebaris.

Pengidentifikasi: IAM_NO_INLINE_POLICY_CHECK

Jenis Sumber Daya: AWS::IAM::User, AWS::IAM::Role, AWS::IAM::Group

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

iam-oidc-provider-tagged

Memeriksa apakah penyedia AWS IAM OIDC memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: IAM_OIDC_PROVIDER_TAGGED

Jenis Sumber Daya: AWS::IAM::OIDCProvider

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Wilayah AS Timur (Virginia Utara)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

iam-password-policy

Memeriksa apakah kebijakan kata sandi akun untuk pengguna AWS Identity and Access Management (IAM) memenuhi persyaratan yang ditentukan yang ditunjukkan dalam parameter. Aturannya adalah NON_COMPLIANT jika kebijakan kata sandi akun tidak memenuhi persyaratan yang ditentukan.

> **Important**
>
> `false`Nilai `true` dan untuk parameter aturan peka huruf besar/kecil. Jika tidak `true` disediakan dalam huruf kecil, itu akan diperlakukan sebagai `false`.

> **Note**
>
> Hasil Evaluasi untuk Kebijakan Kata Sandi IAM Default
>
> Aturan ini ditandai sebagai NON_COMPLIANT ketika kebijakan kata sandi IAM default digunakan.
>
> Aturan Terkelola dan Jenis Sumber Daya IAM Global
>
> Jenis sumber daya IAM global yang tersedia sebelum Februari 2022 (`AWS::IAM::Group`,, `AWS::IAM::PolicyAWS::IAM::Role`, dan`AWS::IAM::User`) hanya dapat direkam oleh AWS Config di AWS Wilayah yang tersedia sebelum AWS Config Februari 2022. Jenis sumber daya ini tidak dapat dicatat di Wilayah yang didukung AWS Config setelah Februari 2022. Untuk daftar Wilayah tersebut, lihat Merekam AWS Sumber Daya | Sumber Daya Global.
>
> Jika Anda merekam jenis sumber daya IAM global di setidaknya satu Wilayah, aturan periodik yang melaporkan kepatuhan pada jenis sumber daya IAM global akan menjalankan evaluasi di semua Wilayah di mana aturan periodik ditambahkan, bahkan jika Anda belum mengaktifkan pencatatan jenis sumber daya IAM global di Wilayah tempat aturan periodik ditambahkan.
>
> Untuk menghindari evaluasi yang tidak perlu, Anda hanya harus menerapkan aturan berkala yang melaporkan kepatuhan pada jenis sumber daya IAM global ke salah satu Wilayah yang didukung. Untuk daftar aturan terkelola yang didukung di Wilayah mana, lihat Daftar Aturan AWS Config Terkelola menurut Ketersediaan Wilayah.

Pengidentifikasi: IAM_PASSWORD_POLICY

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Israel (Tel Aviv), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

RequireUppercaseCharacters (Opsional), Jenis: boolean, Default: betul

Memerlukan setidaknya satu karakter huruf besar dalam kata sandi.

RequireLowercaseCharacters (Opsional), Jenis: boolean, Default: betul

Memerlukan setidaknya satu karakter huruf kecil dalam kata sandi.

RequireSymbols (Opsional), Jenis: boolean, Default: betul

Memerlukan setidaknya satu simbol dalam kata sandi.

RequireNumbers (Opsional), Jenis: boolean, Default: betul

Memerlukan setidaknya satu nomor dalam kata sandi.

MinimumPasswordLength (Opsional), Jenis: int, Default: 14

Panjang minimum kata sandi.

PasswordReusePrevention (Opsional), Jenis: int, Default: 24

Jumlah kata sandi sebelum mengizinkan penggunaan kembali.

MaxPasswordAge (Opsional), Jenis: int, Default: 90

Jumlah hari sebelum kedaluwarsa kata sandi.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

iam-policy-blacklisted-check

Memeriksa di setiap sumber daya AWS Identity and Access Management (IAM), jika kebijakan Amazon Resource Name (ARN) dalam parameter input dilampirkan ke sumber daya IAM. Aturannya adalah NON_COMPLIANT jika kebijakan ARN dilampirkan ke sumber daya IAM.

Pengidentifikasi: IAM_POLICY_BLACKLISTED_CHECK

Jenis Sumber Daya: AWS::IAM::User, AWS::IAM::Group, AWS::IAM::Role

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

policyArns, Jenis: CSV, Default: arn:aws:iam: :aws:policy/ AdministratorAccess

Daftar argumen kebijakan IAM yang dipisahkan koma yang tidak boleh dilampirkan ke entitas IAM mana pun.

ExceptionList (Opsional), Jenis: CSV

Daftar tipe sumber daya yang dipisahkan koma dan daftar pasangan nama sumber daya. Misalnya, pengguna: [user1; user2], grup: [group1; group2], role: [role1; role2; role3].

> **Note**
>
> Untuk daftar pengecualian, tentukan nama sumber daya dan bukan ARN lengkap. Tidak valid:`arn:aws:iam::444455556666:role/Admin`. Berlaku:`Admin`.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

iam-policy-in-use

Memeriksa apakah ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.

> **Note**
>
> Aturan Terkelola dan Jenis Sumber Daya IAM Global
> Jenis sumber daya IAM global yang tersedia sebelum Februari 2022 (`AWS::IAM::Group`,, `AWS::IAM::PolicyAWS::IAM::Role`, dan`AWS::IAM::User`) hanya dapat direkam oleh AWS Config di AWS Wilayah yang tersedia sebelum AWS Config Februari 2022. Jenis sumber daya ini tidak dapat dicatat di Wilayah yang didukung AWS Config setelah Februari 2022. Untuk daftar Wilayah tersebut, lihat [Merekam AWS Sumber Daya | Sumber Daya Global](#).
> Jika Anda merekam jenis sumber daya IAM global di setidaknya satu Wilayah, aturan periodik yang melaporkan kepatuhan pada jenis sumber daya IAM global akan menjalankan evaluasi di semua Wilayah di mana aturan periodik ditambahkan, bahkan jika Anda belum mengaktifkan pencatatan jenis sumber daya IAM global di Wilayah tempat aturan periodik ditambahkan.

Untuk menghindari evaluasi yang tidak perlu, Anda hanya harus menerapkan aturan berkala yang melaporkan kepatuhan pada jenis sumber daya IAM global ke salah satu Wilayah yang didukung. Untuk daftar aturan terkelola yang didukung di Wilayah mana, lihat Daftar Aturan AWS Config Terkelola menurut Ketersediaan Wilayah.

Pengidentifikasi: IAM_POLICY_IN_USE

Jenis Sumber Daya: AWS::IAM::Policy

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

policyARN, Tipe: String

Kebijakan IAM ARN harus diperiksa.

policyUsageType (Opsional), Tipe: String

Tentukan apakah kebijakan tersebut akan dilampirkan ke pengguna, grup, atau peran IAM. Nilai yang valid adalah IAM_USER, IAM_GROUP, IAM_ROLE, atau APAPUN. Nilai default adalah APAPUN.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

iam-policy-no-statements-with-admin-access

Memeriksa apakah kebijakan AWS Identity and Access Management (IAM) yang Anda buat memiliki pernyataan Izinkan yang memberikan izin untuk semua tindakan di semua sumber daya. Aturannya adalah NON_COMPLIANT jika ada pernyataan kebijakan IAM yang dikelola pelanggan menyertakan “Effect”: “Allow” with “Action”: “*” over “Resource”: “*”.

> **Note**
>
> Aturan ini hanya mengevaluasi kebijakan yang dikelola pelanggan. Aturan ini TIDAK mengevaluasi kebijakan inline atau kebijakan AWS terkelola. Untuk informasi selengkapnya tentang perbedaannya, lihat Kebijakan terkelola dan kebijakan sebaris di Panduan Pengguna IAM.

Kebijakan berikut adalah NON_COMPLIANT:

```
"Statement": [
{
"Sid": "VisualEditor",
"Effect": "Allow",
"Action": "*",
"Resource": "*"
}
```

Kebijakan berikut ini sesuai:

```
"Statement": [
{
"Sid": "VisualEditor",
"Effect": "Allow",
"Action": "service:*",
"Resource": "*"
}
```

Pengidentifikasi: IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS

Jenis Sumber Daya: AWS::IAM::Policy

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

excludePermissionBoundaryKebijakan (Opsional), Jenis: boolean

Boolean flag untuk mengecualikan evaluasi kebijakan IAM yang digunakan sebagai batas izin. Jika disetel ke 'true', aturan tidak akan menyertakan batas izin dalam evaluasi. Jika tidak, semua kebijakan IAM dalam lingkup dievaluasi ketika nilai disetel ke 'false.' Nilai default adalah 'salah'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

iam-policy-no-statements-with-full-access

Memeriksa apakah kebijakan AWS Identity and Access Management (IAM) yang Anda buat memberikan izin untuk semua tindakan pada sumber daya individual. AWS Aturannya adalah NON_COMPLIANT jika ada kebijakan IAM yang dikelola pelanggan yang mengizinkan akses penuh ke setidaknya 1 layanan. AWS

Konteks: Mengikuti prinsip hak istimewa terkecil, disarankan untuk membatasi tindakan yang diizinkan dalam kebijakan IAM Anda saat memberikan izin ke layanan. AWS Pendekatan ini membantu memastikan bahwa Anda hanya memberikan izin yang diperlukan dengan menentukan tindakan tepat yang diperlukan, menghindari penggunaan wildcard tidak terbatas untuk layanan, seperti. `ec2:*`

Dalam beberapa kasus, Anda mungkin ingin mengizinkan beberapa tindakan dengan awalan serupa, seperti DescribeFlowLogsdan DescribeAvailabilityZones. Dalam kasus ini, Anda dapat menambahkan wildcard akhiran ke awalan umum (misalnya,). `ec2:Describe*` Mengelompokkan tindakan terkait dapat membantu menghindari mencapai batas ukuran kebijakan IAM.

Aturan ini akan menampilkan COMPLIANT jika Anda menggunakan tindakan awalan dengan wildcard berakhiran (misalnya,). `ec2:Describe*` Aturan ini hanya akan mengembalikan NON_COMPLIANT jika Anda menggunakan wildcard yang tidak dibatasi (misalnya,). `ec2:*`

> **Note**
>
> Aturan ini hanya mengevaluasi kebijakan yang dikelola pelanggan. Aturan ini TIDAK mengevaluasi kebijakan inline atau kebijakan AWS terkelola. Untuk informasi selengkapnya tentang perbedaannya, lihat Kebijakan terkelola dan kebijakan sebaris di Panduan Pengguna IAM.

Pengidentifikasi: IAM_POLICY_NO_STATEMENTS_WITH_FULL_ACCESS

Jenis Sumber Daya: AWS::IAM::Policy

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

excludePermissionBoundaryKebijakan (Opsional), Jenis: boolean

> Boolean flag untuk mengecualikan evaluasi kebijakan IAM yang digunakan sebagai batas izin. Jika disetel ke 'true', aturan tidak akan menyertakan batas izin dalam evaluasi. Jika tidak, semua kebijakan IAM dalam lingkup dievaluasi ketika nilai disetel ke 'false.' Nilai default adalah 'salah'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

iam-role-managed-policy-periksa

Memeriksa apakah semua kebijakan terkelola yang ditentukan dalam daftar kebijakan terkelola dilampirkan ke peran AWS Identity and Access Management (IAM). Aturannya adalah NON_COMPLIANT jika kebijakan terkelola tidak dilampirkan ke peran IAM.

Pengidentifikasi: IAM_ROLE_MANAGED_POLICY_CHECK

Jenis Sumber Daya: AWS::IAM::Role

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

managedPolicyArns, Jenis: CSV

Daftar kebijakan AWS terkelola yang dipisahkan koma Nama Sumber Daya Amazon ()ARNs. Untuk informasi selengkapnya, lihat Nama Sumber Daya Amazon (ARNs) dan kebijakan AWS terkelola di Panduan Pengguna IAM.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

iam-root-access-key-periksa

Memeriksa apakah kunci akses pengguna root tersedia. Aturannya adalah COMPLIANT jika kunci akses pengguna tidak ada. Jika tidak, NON_COMPLIANT.

> **Note**
>
> Aturan Terkelola dan Jenis Sumber Daya IAM Global
>
> Jenis sumber daya IAM global yang tersedia sebelum Februari 2022 (`AWS::IAM::Group`,, `AWS::IAM::Policy`AWS::IAM::Role, dan`AWS::IAM::User`) hanya dapat direkam oleh AWS Config di AWS Wilayah yang tersedia sebelum AWS Config Februari 2022. Jenis sumber daya ini tidak dapat dicatat di Wilayah yang didukung AWS Config setelah Februari 2022. Untuk daftar Wilayah tersebut, lihat Merekam AWS Sumber Daya | Sumber Daya Global.
>
> Jika Anda merekam jenis sumber daya IAM global di setidaknya satu Wilayah, aturan periodik yang melaporkan kepatuhan pada jenis sumber daya IAM global akan menjalankan evaluasi di semua Wilayah di mana aturan periodik ditambahkan, bahkan jika Anda belum mengaktifkan pencatatan jenis sumber daya IAM global di Wilayah tempat aturan periodik ditambahkan.
>
> Untuk menghindari evaluasi yang tidak perlu, Anda hanya harus menerapkan aturan berkala yang melaporkan kepatuhan pada jenis sumber daya IAM global ke salah satu Wilayah yang didukung. Untuk daftar aturan terkelola yang didukung di Wilayah mana, lihat Daftar Aturan AWS Config Terkelola menurut Ketersediaan Wilayah.

Pengidentifikasi: IAM_ROOT_ACCESS_KEY_CHECK

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

iam-saml-provider-tagged

Memeriksa apakah penyedia AWS IAM SALL memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: IAM_SAML_PROVIDER_TAGGED

Jenis Sumber Daya: AWS::IAM::SAMLProvider

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Wilayah AS Timur (Virginia Utara)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

iam-server-certificate-expiration-periksa

Memeriksa apakah sertifikat SSL/TLS server AWS IAM yang disimpan di IAM kedaluwarsa. Aturannya adalah NON_COMPLIANT jika sertifikat server IAM kedaluwarsa.

Pengidentifikasi: IAM_SERVER_CERTIFICATE_EXPIRATION_CHECK

Jenis Sumber Daya: AWS::IAM::ServerCertificate

Jenis pemicu: Berkala

Wilayah AWS: Hanya tersedia di Wilayah AS Timur (Virginia Utara)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

iam-server-certificate-tagged

Memeriksa apakah sertifikat server AWS IAM memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: IAM_SERVER_CERTIFICATE_TAGGED

Jenis Sumber Daya: AWS::IAM::ServerCertificate

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Wilayah AS Timur (Virginia Utara)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

iam-user-group-membership-periksa

Memeriksa apakah pengguna IAM adalah anggota dari setidaknya satu grup IAM.

Pengidentifikasi: IAM_USER_GROUP_MEMBERSHIP_CHECK

Jenis Sumber Daya: AWS::IAM::User

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

GroupNames (Opsional), Tipe: String

Daftar grup IAM yang dipisahkan koma di mana pengguna IAM harus menjadi anggota.

> **Note**
>
> Aturan ini tidak mendukung nama grup dengan koma.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

iam-user-mfa-enabled

Memeriksa apakah pengguna AWS Identity and Access Management (IAM) telah mengaktifkan multi-factor authentication (MFA). Aturannya adalah NON_COMPLIANT jika MFA tidak diaktifkan untuk setidaknya satu pengguna IAM.

> **Note**
>
> Aturan Terkelola dan Jenis Sumber Daya IAM Global
>
> Jenis sumber daya IAM global yang tersedia sebelum Februari 2022 (`AWS::IAM::Group`,, `AWS::IAM::PolicyAWS::IAM::Role`, dan`AWS::IAM::User`) hanya dapat direkam oleh AWS Config di AWS Wilayah yang tersedia sebelum AWS Config Februari 2022. Jenis sumber daya ini tidak dapat dicatat di Wilayah yang didukung AWS Config setelah Februari 2022. Untuk daftar Wilayah tersebut, lihat Merekam AWS Sumber Daya | Sumber Daya Global.
>
> Jika Anda merekam jenis sumber daya IAM global di setidaknya satu Wilayah, aturan periodik yang melaporkan kepatuhan pada jenis sumber daya IAM global akan menjalankan evaluasi di semua Wilayah di mana aturan periodik ditambahkan, bahkan jika Anda belum mengaktifkan pencatatan jenis sumber daya IAM global di Wilayah tempat aturan periodik ditambahkan.
>
> Untuk menghindari evaluasi yang tidak perlu, Anda hanya harus menerapkan aturan berkala yang melaporkan kepatuhan pada jenis sumber daya IAM global ke salah satu Wilayah yang didukung. Untuk daftar aturan terkelola yang didukung di Wilayah mana, lihat Daftar Aturan AWS Config Terkelola menurut Ketersediaan Wilayah.

Pengidentifikasi: IAM_USER_MFA_ENABLED

Jenis Sumber Daya: AWS::IAM::User

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

iam-user-no-policies-periksa

Memeriksa apakah tidak ada pengguna AWS Identity and Access Management (IAM) yang memiliki kebijakan terlampir. Pengguna IAM harus mewarisi izin dari grup atau peran IAM. Aturannya adalah NON_COMPLIANT jika setidaknya ada satu kebijakan yang dilampirkan ke pengguna IAM.

Pengidentifikasi: IAM_USER_NO_POLICIES_CHECK

Jenis Sumber Daya: AWS::IAM::User

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

iam-user-unused-credentials-periksa

Memeriksa apakah pengguna AWS Identity and Access Management (IAM) Anda memiliki kata sandi atau kunci akses aktif yang belum digunakan dalam jumlah hari tertentu yang Anda berikan. Aturannya adalah NON_COMPLIANT jika ada akun tidak aktif yang baru saja digunakan.

> **Note**
>
> Garis Waktu Evaluasi Ulang
> Mengevaluasi ulang aturan ini dalam waktu 4 jam dari evaluasi pertama tidak akan berpengaruh pada hasil.
> Aturan Terkelola dan Jenis Sumber Daya IAM Global
> Jenis sumber daya IAM global yang tersedia sebelum Februari 2022 (`AWS::IAM::Group`,, `AWS::IAM::PolicyAWS::IAM::Role`, dan`AWS::IAM::User`) hanya dapat direkam

oleh AWS Config di AWS Wilayah yang tersedia sebelum AWS Config Februari 2022. Jenis sumber daya ini tidak dapat dicatat di Wilayah yang didukung AWS Config setelah Februari 2022. Untuk daftar Wilayah tersebut, lihat Merekam AWS Sumber Daya | Sumber Daya Global.

Jika Anda merekam jenis sumber daya IAM global di setidaknya satu Wilayah, aturan periodik yang melaporkan kepatuhan pada jenis sumber daya IAM global akan menjalankan evaluasi di semua Wilayah di mana aturan periodik ditambahkan, bahkan jika Anda belum mengaktifkan pencatatan jenis sumber daya IAM global di Wilayah tempat aturan periodik ditambahkan.

Untuk menghindari evaluasi yang tidak perlu, Anda hanya harus menerapkan aturan berkala yang melaporkan kepatuhan pada jenis sumber daya IAM global ke salah satu Wilayah yang didukung. Untuk daftar aturan terkelola yang didukung di Wilayah mana, lihat Daftar Aturan AWS Config Terkelola menurut Ketersediaan Wilayah.

Pengidentifikasi: IAM_USER_UNUSED_CREDENTIALS_CHECK

Jenis Sumber Daya: AWS::IAM::User

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

maxCredentialUsageUmur, Jenis: int, Default: 90

Jumlah hari maksimum kredensi tidak dapat digunakan. Nilai defaultnya adalah 90 hari.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

terbatas-ssh

> **Important**
>
> Untuk aturan ini, pengidentifikasi aturan (INCOMING_SSH_DISABLED) dan nama aturan (restricted-ssh) berbeda.

Memeriksa apakah lalu lintas SSH yang masuk untuk grup keamanan dapat diakses. Aturannya adalah COMPLIANT jika alamat IP dari lalu lintas SSH yang masuk dalam grup keamanan dibatasi (CIDR selain 0.0.0.0/0 atau: :/0). Jika tidak, NON_COMPLIANT.

Pengidentifikasi: INCOMING_SSH_DISABLED

Jenis Sumber Daya: AWS::EC2::SecurityGroup

Jenis pemicu: Perubahan konfigurasi dan Periodik

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

inspector-ec2-scan-enabled

Memeriksa apakah EC2 pemindaian Amazon Inspector V2 diaktifkan untuk lingkungan tunggal atau multi-akun Anda guna mendeteksi potensi kerentanan dan masalah jangkauan jaringan pada instans Anda. EC2 Aturannya adalah NON_COMPLIANT jika EC2 pemindaian tidak diaktifkan.

Pengidentifikasi: EC2 INSPEKTOR_ _SCAN_ENABLED

Jenis Sumber Daya: AWS: :::Akun

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

inspector-ecr-scan-enabled

Memeriksa apakah pemindaian Amazon Inspector V2 ECR diaktifkan untuk lingkungan tunggal atau multi-akun Anda untuk mendeteksi potensi kerentanan perangkat lunak dalam gambar kontainer Anda. Aturannya adalah NON_COMPLIANT jika pemindaian ECR tidak diaktifkan.

Pengidentifikasi: INSPECTOR_ECR_SCAN_ENABLED

Jenis Sumber Daya: AWS: :::Akun

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

inspector-lambda-code-scan-diaktifkan

Memeriksa apakah pemindaian kode Amazon Inspector V2 Lambda diaktifkan untuk lingkungan tunggal atau multi-akun Anda untuk mendeteksi potensi kerentanan kode. Aturannya adalah NON_COMPLIANT jika pemindaian kode Lambda tidak diaktifkan.

Pengidentifikasi: INSPECTOR_LAMBDA_CODE_SCAN_ENABLED

Jenis Sumber Daya: AWS: :::Akun

Jenis pemicu: Berkala

Wilayah AWS: Hanya tersedia di Eropa (Stockholm), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Wilayah Asia Pasifik (Sydney)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

inspector-lambda-standard-scan-diaktifkan

Memeriksa apakah pemindaian standar Amazon Inspector V2 Lambda diaktifkan untuk lingkungan tunggal atau multi-akun Anda untuk mendeteksi potensi kerentanan perangkat lunak. Aturannya adalah NON_COMPLIANT jika pemindaian standar Lambda tidak diaktifkan.

Pengidentifikasi: INSPECTOR_LAMBDA_STANDARD_SCAN_ENABLED

Jenis Sumber Daya: AWS: :::Akun

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ec2- instances-in-vpc

> **Important**
>
> Untuk aturan ini, pengidentifikasi aturan (INSTANCES_IN_VPC) dan nama aturan (ec2-) berbeda. instances-in-vpc

Memeriksa apakah EC2 instance Anda milik virtual private cloud (VPC). Secara opsional, Anda dapat menentukan ID VPC untuk dikaitkan dengan instance Anda.

Pengidentifikasi: INSTANCES_IN_VPC

Jenis Sumber Daya: AWS::EC2::Instance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

vPCid (Opsional), Tipe: String

ID VPC yang berisi instance ini EC2 .

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

internet-gateway-authorized-vpc-hanya

Memeriksa apakah gateway internet dilampirkan ke cloud pribadi virtual resmi (Amazon VPC). Aturannya adalah NON_COMPLIANT jika gateway internet dilampirkan ke VPC yang tidak sah.

Pengidentifikasi: INTERNET_GATEWAY_AUTHORIZED_VPC_ONLY

Jenis Sumber Daya: AWS::EC2::InternetGateway

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

AuthorizedVpcIds (Opsional), Tipe: String

> Daftar IDs VPC resmi yang dipisahkan koma dengan terlampir. IGWs Jika parameter tidak disediakan semua terlampir IGWs akan NON_COMPLIANT.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

iotevents-alarm-model-tagged

Memeriksa apakah model alarm Acara AWS IoT memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: IOTEVENTS_ALARM_MODEL_TAGGED

Jenis Sumber Daya: AWS::IoTEvents::AlarmModel

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Asia Pasifik (Mumbai), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Seoul), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Wilayah Kanada (Tengah)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

iotevents-detector-model-tagged

Memeriksa apakah model detektor Acara AWS IoT memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: IOTEVENTS_DETECTOR_MODEL_TAGGED

Jenis Sumber Daya: AWS::IoTEvents::DetectorModel

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Asia Pasifik (Mumbai), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Seoul), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Wilayah Kanada (Tengah)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

iotevents-input-tagged

Memeriksa apakah input AWS IoT Events memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: IOTEVENTS_INPUT_TAGGED

Jenis Sumber Daya: AWS::IoTEvents::Input

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Asia Pasifik (Mumbai), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Seoul), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Wilayah Kanada (Tengah)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

iotsitewise-asset-model-tagged

Memeriksa apakah model SiteWise aset AWS IoT memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk aturan tersebut. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: IOTSITEWISE_ASSET_MODEL_TAGGED

Jenis Sumber Daya: AWS::IoTSiteWise::AssetModel

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Asia Pasifik (Mumbai), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Seoul), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Wilayah Kanada (Tengah)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

iotsitewise-dashboard-tagged

Memeriksa apakah SiteWise dasbor AWS IoT memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk aturan tersebut. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: IOTSITEWISE_DASHBOARD_TAGGED

Jenis Sumber Daya: AWS::IoTSiteWise::Dashboard

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Asia Pasifik (Mumbai), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Seoul), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Wilayah Kanada (Tengah)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

iotsitewise-gateway-tagged

Memeriksa apakah SiteWise gateway AWS IoT memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk aturan tersebut. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: IOTSITEWISE_GATEWAY_TAGGED

Jenis Sumber Daya: AWS::IoTSiteWise::Gateway

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Asia Pasifik (Mumbai), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Seoul), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Wilayah Kanada (Tengah)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

iotsitewise-portal-tagged

Memeriksa apakah SiteWise portal AWS IoT memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk aturan tersebut. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: IOTSITEWISE_PORTAL_TAGGED

Jenis Sumber Daya: AWS::IoTSiteWise::Portal

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Asia Pasifik (Mumbai), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Seoul), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Wilayah Kanada (Tengah)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

iotsitewise-project-tagged

Memeriksa apakah SiteWise proyek AWS IoT memiliki tag. Secara opsional, Anda dapat menentukan kunci tag untuk aturan tersebut. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: IOTSITEWISE_PROJECT_TAGGED

Jenis Sumber Daya: AWS::IoTSiteWise::Project

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Asia Pasifik (Mumbai), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Seoul), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Wilayah Kanada (Tengah)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

iottwinmaker-component-type-tagged

Memeriksa apakah jenis TwinMaker komponen AWS IoT memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: IOTTWINMAKER_COMPONENT_TYPE_TAGGED

Jenis Sumber Daya: AWS::IoTTwinMaker::ComponentType

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Asia Pasifik (Mumbai), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Seoul), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney) Wilayah

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

iottwinmaker-entity-tagged

Memeriksa apakah TwinMaker entitas AWS IoT memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: IOTTWINMAKER_ENTITY_TAGGED

Jenis Sumber Daya: AWS::IoTTwinMaker::Entity

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), AS Barat (Oregon), Asia Pasifik (Singapura), Wilayah Asia Pasifik (Sydney)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

iottwinmaker-scene-tagged

Memeriksa apakah TwinMaker adegan AWS IoT memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: IOTTWINMAKER_SCENE_TAGGED

Jenis Sumber Daya: AWS::IoTTwinMaker::Scene

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Asia Pasifik (Mumbai), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Seoul), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney) Wilayah

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

iottwinmaker-sync-job-tagged

Memeriksa apakah pekerjaan TwinMaker sinkronisasi AWS IoT memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: IOTTWINMAKER_SYNC_JOB_TAGGED

Jenis Sumber Daya: AWS::IoTTwinMaker::SyncJob

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Asia Pasifik (Mumbai), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Seoul), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney) Wilayah

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

iottwinmaker-workspace-tagged

Memeriksa apakah TwinMaker ruang kerja AWS IoT memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: IOTTWINMAKER_WORKSPACE_TAGGED

Jenis Sumber Daya: AWS::IoTTwinMaker::Workspace

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Asia Pasifik (Mumbai), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Seoul), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney) Wilayah

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

iotwireless-fuota-task-tagged

Memeriksa apakah tugas AWS IoT Wireless FUOTA memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: IOTWIRELESS_FUOTA_TASK_TAGGED

Jenis Sumber Daya: AWS::IoTWireless::FuotaTask

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Eropa (Irlandia), Eropa (Frankfurt), Amerika Selatan (Sao Paulo), AS Timur (Virginia N.), Asia Pasifik (Tokyo), AS Barat (Oregon), Wilayah Asia Pasifik (Sydney)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

iotwireless-multicast-group-tagged

Memeriksa apakah AWS grup multicast IoT Wireless memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: IOTWIRELESS_MULTICAST_GROUP_TAGGED

Jenis Sumber Daya: AWS::IoTWireless::MulticastGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Eropa (Irlandia), Eropa (Frankfurt), Amerika Selatan (Sao Paulo), AS Timur (Virginia N.), Asia Pasifik (Tokyo), AS Barat (Oregon), Wilayah Asia Pasifik (Sydney)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

iotwireless-service-profile-tagged

Memeriksa apakah profil layanan AWS IoT Wireless memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: IOTWIRELESS_SERVICE_PROFILE_TAGGED

Jenis Sumber Daya: AWS::IoTWireless::ServiceProfile

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Eropa (Irlandia), Eropa (Frankfurt), Amerika Selatan (Sao Paulo), AS Timur (Virginia N.), Asia Pasifik (Tokyo), AS Barat (Oregon), Wilayah Asia Pasifik (Sydney)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

iot-authorizer-token-signing-diaktifkan

Memeriksa apakah otorisasi AWS IoT Core belum menonaktifkan persyaratan penandatanganan untuk memvalidasi tanda tangan token dalam permintaan otorisasi. Aturannya adalah NON_COMPLIANT jika otorisasi memiliki konfigurasi. SigningDisabled disetel ke True.

Pengidentifikasi: IOT_AUTHORIZER_TOKEN_SIGNING_ENABLED

Jenis Sumber Daya: AWS::IoT::Authorizer

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Afrika (Cape Town), Asia Pasifik (Hyderabad), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Eropa (Milan), (AS-Timur) AWS GovCloud , (AS-Barat)

AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ivs-channel-playback-authorization-diaktifkan

Memeriksa apakah saluran Amazon IVS mengaktifkan otorisasi pemutaran. Aturannya adalah NON_COMPLIANT jika Configuration.Authorized salah.

Pengidentifikasi: IVS_CHANNEL_PLAYBACK_AUTHORIZATION_ENABLED

Jenis Sumber Daya: AWS::IVS::Channel

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Asia Pasifik (Mumbai), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Seoul), Asia Pasifik (Tokyo), Wilayah AS Barat (Oregon)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ivs-channel-tagged

Memeriksa apakah saluran Amazon IVS memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: IVS_CHANNEL_TAGGED

Jenis Sumber Daya: AWS::IVS::Channel

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Asia Pasifik (Mumbai), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Seoul), Asia Pasifik (Tokyo), Wilayah AS Barat (Oregon)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ivs-playback-key-pair-ditandai

Memeriksa apakah pasangan kunci pemutaran Amazon IVS memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: IVS_PLAYBACK_KEY_PAIR_TAGGED

Jenis Sumber Daya: AWS::IVS::PlaybackKeyPair

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Asia Pasifik (Mumbai), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Seoul), Asia Pasifik (Tokyo), Wilayah AS Barat (Oregon)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ivs-recording-configuration-tagged

Memeriksa apakah konfigurasi perekaman Amazon IVS memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: IVS_RECORDING_CONFIGURATION_TAGGED

Jenis Sumber Daya: AWS::IVS::RecordingConfiguration

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Asia Pasifik (Mumbai), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Seoul), Asia Pasifik (Tokyo), Wilayah AS Barat (Oregon)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

kinesis-firehose-delivery-stream-dienkripsi

Memeriksa apakah aliran pengiriman Amazon Kinesis Data Firehose dienkripsi saat istirahat dengan enkripsi sisi server. Aturannya adalah NON_COMPLIANT jika aliran pengiriman Kinesis Data Firehose tidak dienkripsi saat istirahat dengan enkripsi sisi server.

Pengidentifikasi: KINESIS_FIREHOSE_DELIVERY_STREAM_ENCRYPTED

Jenis Sumber Daya: AWS::KinesisFirehose::DeliveryStream

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

kmsKeyArns (Opsional), Jenis: CSV

Daftar KMS Key Arns yang dipisahkan koma yang disetujui untuk penggunaan Firehose Kinesis.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

kinesis-stream-backup-retention-periksa

Memeriksa apakah Amazon Kinesis Data Stream memiliki periode retensi catatan datanya yang disetel ke jumlah jam tertentu. Aturannya adalah NON_COMPLIANT jika properti RetentionPeriodHours `diatur ke nilai kurang dari nilai yang ditentukan oleh parameter.

Pengidentifikasi: KINESIS_STREAM_BACKUP_RETENTION_CHECK

Jenis Sumber Daya: AWS::Kinesis::Stream

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

minimumBackupRetentionPeriode (Opsional), Tipe: String

Catatan data jam minimum harus disimpan. Nilai yang valid adalah 24 hingga 8760, nilai default adalah 168.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

kinesis-stream-encrypted

Memeriksa apakah aliran Amazon Kinesis dienkripsi saat istirahat dengan enkripsi sisi server. Aturannya adalah NON_COMPLIANT untuk aliran Kinesis jika " StreamEncryption tidak ada.

Konteks: Enkripsi sisi server adalah fitur di Amazon Kinesis Data Streams yang secara otomatis mengenkripsi data sebelum diam dengan menggunakan Kunci KMS. AWS Data dienkripsi sebelum ditulis ke lapisan penyimpanan aliran Kinesis, dan didekripsi setelah diambil dari penyimpanan. Akibatnya, data Anda dienkripsi saat istirahat dalam layanan Kinesis Data Streams. Ini dapat membantu Anda memenuhi persyaratan peraturan dan meningkatkan keamanan data Anda. Untuk informasi selengkapnya, Perlindungan Data di Amazon Kinesis Data Streams.

Pengidentifikasi: KINESIS_STREAM_ENCRYPTED

Jenis Sumber Daya: AWS::Kinesis::Stream

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

kms-cmk-not-scheduled-untuk-penghapusan

Memeriksa apakah AWS kunci Key Management Service (AWS KMS) tidak dijadwalkan untuk dihapus di KMS. AWS Aturannya adalah NON_COMPLIANT jika kunci KMS dijadwalkan untuk dihapus.

Pengidentifikasi: KMS_CMK_NOT_SCHEDULED_FOR_DELETION

Jenis Sumber Daya: AWS::KMS::Key

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Eropa (Milan), Asia Pasifik (Taipei)

Parameter:

kmsKeyIds (Opsional), Tipe: String

> (Opsional) Daftar kunci terkelola pelanggan tertentu yang dipisahkan koma agar IDs tidak dijadwalkan untuk dihapus. Jika Anda tidak menentukan kunci apa pun, aturan memeriksa semua kunci.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

kms-key-policy-no-akses publik

Memeriksa apakah kebijakan kunci AWS KMS memungkinkan akses publik. Aturannya adalah NON_COMPLIANT jika kebijakan kunci KMS mengizinkan akses publik ke kunci KMS.

> **Note**
>
> Agar dianggap non-publik, kebijakan kunci KMS harus memberikan akses hanya ke nilai tetap. [Ini berarti nilai yang tidak mengandung wildcard atau elemen kebijakan IAM berikut: Variabel.](#)

Pengidentifikasi: KMS_KEY_POLICY_NO_PUBLIC_ACCESS

Jenis Sumber Daya: AWS::KMS::Key

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), AWS GovCloud (AS-Timur), AWS GovCloud (AS-Barat), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

lambda-concurrency-check

Memeriksa apakah fungsi Lambda dikonfigurasi dengan batas eksekusi bersamaan tingkat fungsi. Aturannya adalah NON_COMPLIANT jika fungsi Lambda tidak dikonfigurasi dengan batas eksekusi bersamaan tingkat fungsi.

Pengidentifikasi: LAMBDA_CONCURRENCY_CHECK

Jenis Sumber Daya: AWS::Lambda::Function

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei), Tiongkok (Ningxia)

Parameter:

ConcurrencyLimitLow (Opsional), Tipe: String

Batas eksekusi konkurensi minimum

ConcurrencyLimitHigh (Opsional), Tipe: String

Batas eksekusi konkurensi maksimum

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

lambda-dlq-check

Memeriksa apakah fungsi Lambda dikonfigurasi dengan antrian huruf mati. Aturannya adalah NON_COMPLIANT jika fungsi Lambda tidak dikonfigurasi dengan antrian huruf mati.

Pengidentifikasi: LAMBDA_DLQ_CHECK

Jenis Sumber Daya: AWS::Lambda::Function

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei), Tiongkok (Ningxia)

Parameter:

DlQarns (Opsional), Tipe: String

> Daftar Amazon SQS dan Amazon ARNs SNS yang dipisahkan koma yang harus dikonfigurasi sebagai target antrian huruf mati fungsi Lambda.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

lambda-function-public-access-dilarang

Memeriksa apakah kebijakan AWS Lambda fungsi yang dilampirkan pada sumber daya Lambda melarang akses publik. Jika kebijakan fungsi Lambda mengizinkan akses publik, itu adalah NON_COMPLIANT.

Konteks: Kebijakan fungsi lambda dianggap mengizinkan akses publik jika elemen utama kosong atau berisi wildcard. Misalnya, jika elemen utama adalah `“”` atau`{“AWS”: “”}`. Pemberian akses publik tidak disarankan untuk alasan keamanan. Membatasi akses publik dapat membantu Anda mencegah pemanggilan fungsi Lambda Anda yang tidak sah, yang dapat membahayakan data Anda atau menimbulkan biaya yang tidak diinginkan.

Untuk membatasi akses ke fungsi Lambda Anda, tentukan AWS IDs akun atau Nama Sumber Daya Amazon ARNs () pengguna, peran, atau layanan IAM yang dapat memanggil fungsi tersebut. Untuk

informasi selengkapnya, lihat Memberikan akses fungsi ke akun lain di Panduan AWS Lambda Pengembang.

Aturannya juga `NON_COMPLIANT` jika fungsi Lambda dipanggil dari Amazon S3, dan kebijakan tersebut tidak menyertakan kondisi untuk membatasi akses publik, seperti. `AWS:SourceAccount` Sebaiknya gunakan kondisi S3 lainnya beserta `AWS:SourceAccount` kebijakan bucket Anda untuk akses yang lebih disempurnakan.

> **Note**
>
> Agar dianggap non-publik, kebijakan berbasis sumber daya Lambda harus memberikan akses hanya ke nilai tetap. Ini berarti nilai yang tidak mengandung wildcard atau elemen kebijakan IAM berikut: Variabel.

Pengidentifikasi: LAMBDA_FUNCTION_PUBLIC_ACCESS_FORBIDNED

Jenis Sumber Daya: AWS::Lambda::Function

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Eropa (Spanyol), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

lambda-function-settings-check

Memeriksa apakah setelan fungsi AWS Lambda untuk runtime, role, timeout, dan ukuran memori cocok dengan nilai yang diharapkan. Aturan mengabaikan fungsi dengan tipe paket 'Gambar' dan fungsi dengan runtime disetel ke 'OS-Only Runtime'. Aturannya adalah NON_COMPLIANT jika pengaturan fungsi Lambda tidak cocok dengan nilai yang diharapkan.

Pengidentifikasi: LAMBDA_FUNCTION_SETTINGS_CHECK

Jenis Sumber Daya: AWS::Lambda::Function

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Tiongkok (Ningxia)

Parameter:

runtime, Jenis: CSV

Daftar nilai runtime Lambda AWS yang dipisahkan koma

peran (Opsional), Tipe: String

Nama atau ARN dari peran eksekusi Lambda AWS

batas waktu (Opsional), Jenis: int, Default: 3

AWS Batas waktu fungsi Lambda dalam hitungan detik

MemorySize (Opsional), Jenis: int, Default: 128

AWS Ukuran fungsi Lambda dalam megabyte

Evaluasi Proaktif

Untuk langkah-langkah tentang cara menjalankan aturan ini dalam mode proaktif, lihat Mengevaluasi Sumber Daya Anda dengan AWS Config Aturan. Agar aturan ini mengembalikan COMPLIANT dalam mode proaktif, skema konfigurasi sumber daya untuk StartResourceEvaluationAPI harus menyertakan input berikut, yang dikodekan sebagai string:

```
"ResourceConfiguration":
...
{
    "MemorySize": Integer*,
    "Role": String*,
    "Runtime": String*,
    "Timeout": Integer*
}
...
```

* Untuk informasi selengkapnya tentang nilai valid untuk input ini, lihat, Peran MemorySize, Runtime, dan Timeout di Panduan Pengguna. AWS CloudFormation

Untuk informasi lebih lanjut tentang evaluasi proaktif, lihat Mode Evaluasi.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

lambda-function-xray-enabled

Memeriksa apakah AWS X-Ray diaktifkan pada fungsi AWS Lambda. Aturannya NON_COMPLIANT jika penelusuran X-Ray dinonaktifkan untuk fungsi Lambda.

Pengidentifikasi: LAMBDA_FUNCTION_XRAY_ENABLED

Jenis Sumber Daya: AWS::Lambda::Function

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Seoul), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

lambda-inside-vpc

Memeriksa apakah fungsi Lambda diizinkan akses ke cloud pribadi virtual (VPC). Aturannya adalah NON_COMPLIANT jika fungsi Lambda tidak diaktifkan VPC.

Pengidentifikasi: LAMBDA_INSIDE_VPC

Jenis Sumber Daya: AWS::Lambda::Function

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Tiongkok (Ningxia)

Parameter:

SubnetiDs (Opsional), Tipe: String

Daftar Subnet yang dipisahkan koma yang dapat dikaitkan dengan fungsi IDs Lambda.

Evaluasi Proaktif

Untuk langkah-langkah tentang cara menjalankan aturan ini dalam mode proaktif, lihat Mengevaluasi Sumber Daya Anda dengan AWS Config Aturan. Agar aturan ini mengembalikan COMPLIANT dalam mode proaktif, skema konfigurasi sumber daya untuk StartResourceEvaluationAPI harus menyertakan input berikut, yang dikodekan sebagai string:

```
"ResourceConfiguration":
...
{
   "VpcConfig": {
         "SubnetIds": "[SubnetId-1, SubnetId-2, SubnetId-3, ...]"
   }
}
...
```

Untuk informasi lebih lanjut tentang evaluasi proaktif, lihat Mode Evaluasi.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

lambda-vpc-multi-az-periksa

Memeriksa apakah Lambda memiliki lebih dari 1 zona ketersediaan terkait. Aturannya adalah NON_COMPLIANT jika hanya 1 zona ketersediaan yang dikaitkan dengan Lambda atau jumlah zona ketersediaan yang terkait kurang dari jumlah yang ditentukan dalam parameter opsional.

Pengidentifikasi: LAMBDA_VPC_MULTI_AZ_CHECK

Jenis Sumber Daya: AWS::Lambda::Function

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur), AWS GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), China (Ningxia) Wilayah

Parameter:

AvailabilityZones (Opsional), Jenis: int

Jumlah zona Ketersediaan yang diharapkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

lightsail-bucket-tagged

Memeriksa apakah ember Amazon Lightsail memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: LIGHTSAIL_BUCKET_TAGGED

Jenis Sumber Daya: AWS::Lightsail::Bucket

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Eropa (Stockholm), Asia Pasifik (Mumbai), Eropa (Paris), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Seoul), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Kanada (Tengah) Wilayah

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

lightsail-certificate-tagged

Memeriksa apakah sertifikat Amazon Lightsail memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: LIGHTSAIL_CERTIFICATE_TAGGED

Jenis Sumber Daya: AWS::Lightsail::Certificate

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Eropa (Stockholm), Asia Pasifik (Mumbai), Eropa (Paris), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Seoul), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Kanada (Tengah) Wilayah

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

lightsail-disk-tagged

Memeriksa apakah disk Amazon Lightsail memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: LIGHTSAIL_DISK_TAGGED

Jenis Sumber Daya: AWS::Lightsail::Disk

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Eropa (Stockholm), Asia Pasifik (Mumbai), Eropa (Paris), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N.), Asia Pasifik (Seoul), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Kanada (Tengah) Wilayah

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

macie-auto-sensitive-data-penemuan-cek

Memeriksa apakah penemuan data sensitif otomatis diaktifkan untuk Amazon Macie. Aturannya adalah NON_COMPLIANT jika penemuan data sensitif otomatis dinonaktifkan. Aturan ini BERLAKU untuk akun administrator dan NOT_APPLICABLE untuk akun anggota.

Pengidentifikasi: MACIE_AUTO_SENSITIVE_DATA_DISCOVERY_CHECK

Jenis Sumber Daya: AWS: :::Akun

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok Wilayah (Ningxia), Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

macie-status-check

Memeriksa apakah Amazon Macie diaktifkan di akun Anda per wilayah. Aturannya adalah NON_COMPLIANT jika atribut 'status' tidak disetel ke 'ENABLED'.

Pengidentifikasi: MACIE_STATUS_CHECK

Jenis Sumber Daya: AWS: :::Akun

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

mariadb-publish-logs-to-cloudwatch-log

Memeriksa apakah instance database Amazon MariaDB dikonfigurasi untuk mempublikasikan log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika instance database tidak dikonfigurasi untuk mempublikasikan log ke Log. CloudWatch

Pengidentifikasi: MARIADB_PUBLISH_LOGS_TO_CLOUDWATCH_LOGS

Jenis Sumber Daya: AWS::RDS::DBInstance

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (Bahrain), Tiongkok (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

LogTypes (Opsional), Tipe: String

> Daftar tipe log yang dipisahkan koma untuk diperiksa aturan. Jika tidak disediakan, aturan akan memeriksa jenis log default: 'error' dan 'audit'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

mfa-enabled-for-iam-akses konsol

Memeriksa apakah otentikasi AWS multi-faktor (MFA) diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) yang menggunakan kata sandi konsol. Aturannya adalah COMPLIANT jika MFA diaktifkan.

> **Note**
>
> Garis Waktu Evaluasi Ulang
> Mengevaluasi ulang aturan ini dalam waktu 4 jam dari evaluasi pertama tidak akan berpengaruh pada hasil.
> Aturan Terkelola dan Jenis Sumber Daya IAM Global
> Jenis sumber daya IAM global yang tersedia sebelum Februari 2022 (`AWS::IAM::Group`,, `AWS::IAM::PolicyAWS::IAM::Role`, dan`AWS::IAM::User`) hanya dapat direkam oleh AWS Config di AWS Wilayah yang tersedia sebelum AWS Config Februari 2022. Jenis sumber daya ini tidak dapat dicatat di Wilayah yang didukung AWS Config setelah Februari 2022. Untuk daftar Wilayah tersebut, lihat [Merekam AWS Sumber Daya | Sumber Daya Global](#).
> Jika Anda merekam jenis sumber daya IAM global di setidaknya satu Wilayah, aturan periodik yang melaporkan kepatuhan pada jenis sumber daya IAM global akan menjalankan evaluasi di semua Wilayah di mana aturan periodik ditambahkan, bahkan jika Anda belum

mengaktifkan pencatatan jenis sumber daya IAM global di Wilayah tempat aturan periodik ditambahkan.
Untuk menghindari evaluasi yang tidak perlu, Anda hanya harus menerapkan aturan berkala yang melaporkan kepatuhan pada jenis sumber daya IAM global ke salah satu Wilayah yang didukung. Untuk daftar aturan terkelola yang didukung di Wilayah mana, lihat Daftar Aturan AWS Config Terkelola menurut Ketersediaan Wilayah.

Pengidentifikasi: MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS

Jenis Sumber Daya: AWS::IAM::User

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

mq-active-broker-ldap-otentikasi

Memeriksa apakah broker Amazon MQ ActiveMQ menggunakan strategi otentikasi LDAP untuk mengamankan broker. Aturannya adalah NON_COMPLIANT jika konfigurasi. AuthenticationStrategy bukan 'ldap'.

Pengidentifikasi: MQ_ACTIVE_BROKER_LDAP_AUTHENTICATION

Jenis Sumber Daya: AWS::AmazonMQ::Broker

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS

GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Eropa (Zen Wilayah)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

mq-active-deployment-mode

Memeriksa mode penerapan yang dikonfigurasi untuk mesin broker Amazon MQ ActiveMQ. Aturannya adalah NON_COMPLIANT jika mode broker instans tunggal default sedang digunakan.

Pengidentifikasi: MQ_ACTIVE_DEPLOYMENT_MODE

Jenis Sumber Daya: AWS::AmazonMQ::Broker

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), AWS GovCloud (AS-Timur), (AS-Barat), Meksiko AWS GovCloud (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

mq-active-single-instance-broker-storage-type-efs

Memeriksa apakah Amazon MQ untuk broker instans tunggal ActiveMQ menggunakan keluarga tipe instans mq.m5 dikonfigurasi dengan Amazon Elastic File System (EFS) untuk penyimpanan broker. Aturannya adalah NON_COMPLIANT jika konfigurasi. StorageType bukan 'efs'.

Pengidentifikasi: MQ_ACTIVE_SINGLE_INSTANCE_BROKER_STORAGE_TYPE_EFS

Jenis Sumber Daya: AWS::AmazonMQ::Broker

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Eropa (Zen Wilayah)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

mq-automatic-minor-version-upgrade diaktifkan

Memeriksa apakah upgrade versi minor otomatis diaktifkan untuk broker Amazon MQ. Aturannya adalah NON_COMPLIANT jika bidang AutoMinorVersionUpgrade '' tidak diaktifkan untuk broker Amazon MQ.

Pengidentifikasi: MQ_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED

Jenis Sumber Daya: AWS::AmazonMQ::Broker

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Afrika (Cape Town), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

mq-auto-minor-version-upgrade diaktifkan

Memeriksa apakah upgrade versi minor otomatis diaktifkan untuk broker Amazon MQ. Aturannya adalah NON_COMPLIANT jika bidang AutoMinorVersionUpgrade " tidak diaktifkan untuk broker Amazon MQ.

Pengidentifikasi: MQ_AUTO_MINOR_VERSION_UPGRADE_ENABLED

Jenis Sumber Daya: AWS::AmazonMQ::Broker

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), AWS GovCloud (AS-Timur), (AS-Barat), Meksiko AWS GovCloud (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

mq-broker-general-logging-diaktifkan

Memeriksa apakah broker Amazon MQ mengaktifkan pencatatan umum. Aturannya adalah NON_COMPLIANT jika Configuration.logs.general salah.

Pengidentifikasi: MQ_BROKER_GENERAL_LOGGING_ENABLED

Jenis Sumber Daya: AWS::AmazonMQ::Broker

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Eropa (Zen Wilayah)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

mq-cloudwatch-audit-logging-diaktifkan

Memeriksa apakah broker Amazon MQ mengaktifkan pencatatan CloudWatch audit Amazon. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.

Pengidentifikasi: MQ_CLOUDWATCH_AUDIT_LOGGING_ENABLED

Jenis Sumber Daya: AWS::AmazonMQ::Broker

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Afrika (Cape Town), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

mq-cloudwatch-audit-log-diaktifkan

Memeriksa apakah broker Amazon MQ mengaktifkan pencatatan CloudWatch audit. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.

Pengidentifikasi: MQ_CLOUDWATCH_AUDIT_LOG_ENABLED

Jenis Sumber Daya: AWS::AmazonMQ::Broker

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

mq-no-public-access

Memeriksa apakah broker Amazon MQ tidak dapat diakses publik. Aturannya adalah NON_COMPLIANT jika bidang 'PubliclyAccessible' disetel ke true untuk broker Amazon MQ.

Pengidentifikasi: MQ_NO_PUBLIC_ACCESS

Jenis Sumber Daya: AWS::AmazonMQ::Broker

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Afrika (Cape Town), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

mq-rabbit-deployment-mode

Memeriksa mode penerapan yang dikonfigurasi untuk mesin broker Amazon MQ RabbitMQ. Aturannya adalah NON_COMPLIANT jika mode broker instans tunggal default sedang digunakan.

Pengidentifikasi: MQ_RABBIT_DEPLOYMENT_MODE

Jenis Sumber Daya: AWS::AmazonMQ::Broker

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur), AWS GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

msk-cluster-public-access-dinonaktifkan

Memeriksa apakah akses publik dinonaktifkan di klaster MSK Amazon. Aturannya adalah NON_COMPLIANT jika akses publik di klaster MSK Amazon tidak dinonaktifkan.

Pengidentifikasi: MSK_CLUSTER_PUBLIC_ACCESS_DISABLED

Jenis Sumber Daya: AWS::MSK::Cluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Seoul), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

msk-connect-connector-logging-diaktifkan

Memeriksa apakah Amazon MSK Connector telah mengaktifkan logging ke salah satu tujuan log. Aturannya adalah NON_COMPLIANT jika Amazon MSK Connector tidak mengaktifkan logging.

Pengidentifikasi: MSK_CONNECT_CONNECTOR_LOGGING_ENABLED

Jenis Sumber Daya: AWS::KafkaConnect::Connector

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Eropa (Stockholm), Asia Pasifik (Mumbai), Eropa (Paris), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), Amerika Selatan (Sao Paulo), AS Timur (Virginia N.), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), AS Barat (California N.), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Wilayah Kanada (Tengah)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

msk-enhanced-monitoring-enabled

Memeriksa apakah pemantauan yang disempurnakan diaktifkan untuk kluster MSK Amazon yang disetel ke PER_TOPIC_PER_BROKER atau PER_TOPIC_PER_PARTITION. Aturannya adalah NON_COMPLIANT jika pemantauan yang ditingkatkan diaktifkan dan disetel ke DEFAULT atau PER_BROKER.

Pengidentifikasi: MSK_ENHANCED_MONITORING_ENABLED

Jenis Sumber Daya: AWS::MSK::Cluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur), AWS GovCloud AWS GovCloud (AS-Barat), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

msk-in-cluster-node-membutuhkan-tls

Memeriksa apakah klaster MSK Amazon memberlakukan enkripsi dalam perjalanan menggunakan HTTPS (TLS) dengan node broker cluster. Aturannya adalah NON_COMPLIANT jika komunikasi teks biasa diaktifkan untuk koneksi node broker in-cluster.

Pengidentifikasi: MSK_IN_CLUSTER_NODE_REQUIRE_TLS

Jenis Sumber Daya: AWS::MSK::Cluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur), AWS GovCloud AWS GovCloud (AS-Barat), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

msk-unrestricted-access-check

Memeriksa apakah Cluster MSK Amazon memiliki akses yang tidak diautentikasi dinonaktifkan. Aturannya adalah NON_COMPLIANT jika Amazon MSK Cluster mengaktifkan akses yang tidak diautentikasi.

Pengidentifikasi: MSK_UNRESTRICTED_ACCESS_CHECK

Jenis Sumber Daya: AWS::MSK::Cluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Seoul), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

multi-region-cloudtrail-enabled

> **Important**
>
> Untuk aturan ini, pengidentifikasi aturan (MULTI_REGION_CLOUD_TRAIL_ENABLED) dan nama aturan () berbeda. multi-region-cloudtrail-enabled

Memeriksa apakah ada setidaknya satu multi-wilayah AWS CloudTrail. Aturannya adalah NON_COMPLIANT jika jejak tidak cocok dengan parameter input. Aturannya adalah NON_COMPLIANT jika `ExcludeManagementEventSources` bidang tidak kosong atau jika AWS CloudTrail dikonfigurasi untuk mengecualikan peristiwa manajemen seperti peristiwa AWS KMS atau peristiwa Amazon RDS Data API.

Pengidentifikasi: MULTI_REGION_CLOUD_TRAIL_ENABLED

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

s3 BucketName (Opsional), Tipe: String

Nama bucket Amazon S3 untuk mengirimkan file log AWS CloudTrail ke.

snsTopicArn (Opsional), Tipe: String

Amazon SNS topik ARN untuk digunakan AWS CloudTrail untuk notifikasi.

cloudWatchLogsLogGroupArn (Opsional), Tipe: String

Grup CloudWatch log Amazon ARN untuk mengirim data AWS CloudTrail ke.

includeManagementEvents (Opsional), Jenis: boolean

Pemilih acara untuk memasukkan acara manajemen untuk. AWS CloudTrail

readWriteType (Opsional), Tipe: String

Jenis acara untuk direkam. Nilai yang valid adalah ReadOnly, WriteOnly dan SEMUA.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

nacl-no-unrestricted-ssh-rdp

Memeriksa apakah port default untuk SSH/RDP lalu lintas masuk untuk daftar kontrol akses jaringan (NACLs) tidak dibatasi. Aturannya adalah NON_COMPLIANT jika entri masuk NACL memungkinkan blok sumber TCP atau UDP CIDR untuk port 22 atau 3389.

Pengidentifikasi: NACL_NO_UNRESTRICTED_SSH_RDP

Jenis Sumber Daya: AWS::EC2::NetworkAcl

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

neptune-cluster-backup-retention-periksa

Memeriksa apakah periode retensi klaster Amazon Neptunus DB disetel ke jumlah hari tertentu. Aturannya adalah NON_COMPLIANT jika periode retensi kurang dari nilai yang ditentukan oleh parameter.

Pengidentifikasi: NEPTUNE_CLUSTER_BACKUP_RETENTION_CHECK

Jenis Sumber Daya: AWS::RDS::DBCluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Eropa (Milan), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Eropa (Zurich) Wilayah

Parameter:

minimumBackupRetentionPeriode (Opsional), Jenis: int

> Backup hari minimum harus disimpan. Nilai valid 1 hingga 35, nilai default adalah 7. Aturannya adalah NON_COMPLIANT jika nilainya lebih besar dari ". backupRetentionPeriod Aturannya adalah COMPLIANT jika nilainya kurang dari atau sama dengan 'backupRetentionPeriod'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

neptune-cluster-cloudwatch-log-ekspor diaktifkan

Memeriksa apakah klaster CloudWatch Amazon Neptunus mengaktifkan ekspor log untuk log audit. Aturannya adalah NON_COMPLIANT jika klaster Neptunus tidak mengaktifkan ekspor log untuk log audit. CloudWatch

Pengidentifikasi: NEPTUNE_CLUSTER_CLOUDWATCH_LOG_EXPORT_ENABLED

Jenis Sumber Daya: AWS::RDS::DBCluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Eropa (Milan), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Eropa (Zurich) Wilayah

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

neptune-cluster-copy-tags-to-snapshot-enabled

Memeriksa apakah kluster Amazon Neptunus dikonfigurasi untuk menyalin semua tag ke snapshot saat snapshot dibuat. Aturannya adalah NON_COMPLIANT jika 'copyTagsToSnapshot' disetel ke false.

Pengidentifikasi: NEPTUNE_CLUSTER_COPY_TAGS_TO_SNAPSHOT_ENABLED

Jenis Sumber Daya: AWS::RDS::DBCluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Eropa (Milan), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Eropa (Zurich) Wilayah

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

neptune-cluster-deletion-protection-diaktifkan

Memeriksa apakah klaster Amazon Neptunus DB memiliki perlindungan penghapusan yang diaktifkan. Aturannya adalah NON_COMPLIANT jika klaster Amazon Neptunus memiliki bidang DeletionProtection disetel ke false.

Pengidentifikasi: NEPTUNE_CLUSTER_DELETION_PROTECTION_ENABLED

Jenis Sumber Daya: AWS::RDS::DBCluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Eropa (Milan), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Eropa (Zurich) Wilayah

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

neptune-cluster-encrypted

Memeriksa apakah enkripsi penyimpanan diaktifkan untuk kluster Amazon Neptunus DB Anda. Aturannya adalah NON_COMPLIANT jika enkripsi penyimpanan tidak diaktifkan.

Pengidentifikasi: NEPTUNE_CLUSTER_ENCRYPTED

Jenis Sumber Daya: AWS::RDS::DBCluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Eropa (Milan), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Eropa (Zurich) Wilayah

Parameter:

KmsKeyArns (Opsional), Jenis: CSV

> Daftar kunci KMS yang dipisahkan koma ARNs untuk dibandingkan dengan cluster KmsKeyId terenkripsi.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

neptune-cluster-iam-database-otentikasi

Memeriksa apakah klaster AWS Amazon Neptune mengaktifkan otentikasi basis data Identity and Access Management (IAM) and Access Management (IAM). Aturannya adalah NON_COMPLIANT jika klaster Amazon Neptunus tidak mengaktifkan autentikasi database IAM.

Pengidentifikasi: NEPTUNE_CLUSTER_IAM_DATABASE_AUTHENTICATION

Jenis Sumber Daya: AWS::RDS::DBCluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne),

Eropa (Milan), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Eropa (Zurich) Wilayah

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

neptune-cluster-multi-az-diaktifkan

Memeriksa apakah cluster Amazon Neptunus dikonfigurasi dengan replikasi Amazon RDS Multi-AZ. Aturannya adalah NON_COMPLIANT jika replikasi multi-AZ tidak diaktifkan.

Pengidentifikasi: NEPTUNE_CLUSTER_MULTI_AZ_ENABLED

Jenis Sumber Daya: AWS::RDS::DBCluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Eropa (Milan), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Eropa (Zurich) Wilayah

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

neptune-cluster-snapshot-encrypted

Memeriksa apakah cluster Amazon Neptunus DB memiliki snapshot yang dienkripsi. Aturannya adalah NON_COMPLIANT jika cluster Neptunus tidak memiliki snapshot yang dienkripsi.

Pengidentifikasi: NEPTUNE_CLUSTER_SNAPSHOT_ENCRYPTED

Jenis Sumber Daya: AWS::RDS::DBClusterSnapshot

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Eropa (Milan), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

neptune-cluster-snapshot-public-dilarang

Memeriksa apakah snapshot cluster DB manual Amazon Neptunus bersifat publik. Aturannya adalah NON_COMPLIANT jika ada snapshot cluster Neptunus yang ada dan yang baru bersifat publik.

Pengidentifikasi: NEPTUNE_CLUSTER_SNAPSHOT_PUBLIC_FORBIDNED

Jenis Sumber Daya: AWS::RDS::DBClusterSnapshot

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Eropa (Milan), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

netfw-deletion-protection-enabled

Memeriksa apakah AWS Network Firewall memiliki perlindungan penghapusan yang diaktifkan. Aturannya adalah NON_COMPLIANT jika Network Firewall tidak mengaktifkan proteksi penghapusan.

Pengidentifikasi: NETFW_DELETION_PROTECTION_ENABLED

Jenis Sumber Daya: AWS::NetworkFirewall::Firewall

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Tiongkok (Ningxia) Wilayah

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

netfw-logging-enabled

Memeriksa apakah firewall AWS Network Firewall telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika jenis logging tidak dikonfigurasi. Anda dapat menentukan jenis logging yang Anda ingin aturan untuk memeriksa.

Pengidentifikasi: NETFW_LOGGING_ENABLED

Jenis Sumber Daya: AWS::NetworkFirewall::LoggingConfiguration

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Tiongkok (Ningxia) Wilayah

Parameter:

LogType (Opsional), Tipe: String

> LogType (Opsional): Jenis log untuk aturan untuk memeriksa firewall: 'alert', 'flow', atau 'keduanya'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

netfw-multi-az-enabled

Memeriksa apakah firewall AWS Network Firewall digunakan di beberapa Availability Zone. Aturannya adalah NON_COMPLIANT jika firewall dikerahkan hanya di satu Availability Zone atau di zona yang lebih sedikit daripada nomor yang tercantum dalam parameter opsional.

Pengidentifikasi: NETFW_MULTI_AZ_ENABLED

Jenis Sumber Daya: AWS::NetworkFirewall::Firewall

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Tiongkok (Ningxia) Wilayah

Parameter:

AvailabilityZones (Opsional), Jenis: int

> Jumlah Availability Zone yang diharapkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

netfw-policy-default-action-fragmen-paket

Memeriksa apakah kebijakan AWS Network Firewall dikonfigurasi dengan tindakan default stateless yang ditentukan pengguna untuk paket yang terfragmentasi. Aturannya adalah NON_COMPLIANT jika tindakan default stateless untuk paket terfragmentasi tidak cocok dengan tindakan default yang ditentukan pengguna.

Pengidentifikasi: NETFW_POLICY_DEFAULT_ACTION_FRAGMENT_PACKETS

Jenis Sumber Daya: AWS::NetworkFirewall::FirewallPolicy

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Tiongkok (Ningxia) Wilayah

Parameter:

statelessFragmentDefaultTindakan, Jenis: CSV

> Daftar nilai yang dipisahkan koma. Anda dapat memilih maksimal dua. Nilai yang valid termasuk 'aws:pass', 'aws:drop', dan 'aws:forward_to_sfe'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

netfw-policy-default-action-paket penuh

Memeriksa apakah kebijakan AWS Network Firewall dikonfigurasi dengan tindakan stateless default yang ditentukan pengguna untuk paket lengkap. Aturan ini adalah NON_COMPLIANT jika tindakan stateless default untuk paket lengkap tidak cocok dengan tindakan stateless default yang ditentukan pengguna.

Pengidentifikasi: NETFW_POLICY_DEFAULT_ACTION_FULL_PACKETS

Jenis Sumber Daya: AWS::NetworkFirewall::FirewallPolicy

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Tiongkok (Ningxia) Wilayah

Parameter:

statelessDefaultActions, Jenis: CSV

> Daftar nilai yang dipisahkan koma. Anda dapat memilih maksimal dua. Nilai yang valid termasuk 'aws:pass', 'aws:drop', dan 'aws:forward_to_sfe'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

netfw-policy-rule-group-terkait

Kebijakan Check AWS Network Firewall dikaitkan dengan grup aturan stateful ATAU stateless. Aturan ini adalah NON_COMPLIANT jika tidak ada grup aturan stateful atau stateless yang terkait dengan kebijakan Network Firewall else COMPLIANT jika salah satu grup aturan ada.

Pengidentifikasi: NETFW_POLICY_RULE_GROUP_ASSOCIATED

Jenis Sumber Daya: AWS::NetworkFirewall::FirewallPolicy

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

netfw-stateless-rule-group-tidak-kosong

Memeriksa apakah Grup Aturan Firewall Jaringan Stateless berisi aturan. Aturannya adalah NON_COMPLIANT jika tidak ada aturan dalam Grup Aturan Firewall Jaringan Stateless.

Pengidentifikasi: NETFW_STATELESS_RULE_GROUP_NOT_EMPTY

Jenis Sumber Daya: AWS::NetworkFirewall::RuleGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

netfw-subnet-change-protection-diaktifkan

Memeriksa apakah AWS Network Firewall memiliki perlindungan perubahan subnet yang diaktifkan. Aturannya adalah NON_COMPLIANT jika perlindungan perubahan subnet tidak diaktifkan.

Pengidentifikasi: NETFW_SUBNET_CHANGE_PROTECTION_ENABLED

Jenis Sumber Daya: AWS::NetworkFirewall::Firewall

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (Bahrain), Tiongkok (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

nlb-cross-zone-load-menyeimbangkan diaktifkan

Memeriksa apakah penyeimbangan beban lintas zona diaktifkan pada Network Load Balancers (). NLBs Aturannya adalah NON_COMPLIANT jika penyeimbangan beban lintas zona tidak diaktifkan untuk NLB.

Pengidentifikasi: NLB_CROSS_ZONE_LOAD_BALANCING_ENABLED

Jenis Sumber Daya: AWS::ElasticLoadBalancingV2::LoadBalancer

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

nlb-internal-scheme-check

Memeriksa apakah skema Network Load Balancer bersifat internal. Aturannya adalah NON_COMPLIANT jika configuration.scheme tidak disetel ke internal.

Pengidentifikasi: NLB_INTERNAL_SCHEME_CHECK

Jenis Sumber Daya: AWS::ElasticLoadBalancingV2::LoadBalancer

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

nlb-listener-tagged

Memeriksa apakah pendengar Network Load Balancer memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: NLB_LISTENER_TAGGED

Jenis Sumber Daya: AWS::ElasticLoadBalancingV2::Listener

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

nlb-logging-enabled

Memeriksa apakah pencatatan akses diaktifkan untuk Network Load Balancers. Aturannya adalah NON_COMPLIANT jika pencatatan akses tidak diaktifkan untuk penyeimbang Beban Jaringan.

Pengidentifikasi: NLB_LOGGING_ENABLED

Jenis Sumber Daya: AWS::ElasticLoadBalancingV2::LoadBalancer

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

no-unrestricted-route-to-igw

Memeriksa apakah ada rute umum dalam tabel rute ke gateway Internet (IGW). Aturannya adalah NON_COMPLIANT jika rute ke IGW memiliki blok CIDR tujuan '0.0.0.0/0' atau ': :/0' atau jika blok CIDR tujuan tidak cocok dengan parameter aturan.

Pengidentifikasi: NO_UNRESTRICTED_ROUTE_TO_IGW

Jenis Sumber Daya: AWS::EC2::RouteTable

Jenis pemicu: Perubahan konfigurasi dan Periodik

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei), Kanada Barat (Calgary)

Parameter:

routeTableIds (Opsional), Jenis: CSV

Daftar tabel rute yang dipisahkan koma IDs yang dapat memiliki rute ke Internet Gateway dengan blok CIDR tujuan '0.0.0.0/0' atau ': :/0'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

opensearch-access-control-enabled

Memeriksa apakah domain OpenSearch Layanan Amazon mengaktifkan kontrol akses berbutir halus. Aturannya adalah NON_COMPLIANT jika tidak AdvancedSecurityOptions diaktifkan untuk domain Layanan. OpenSearch

Pengidentifikasi: OPENSEARCH_ACCESS_CONTROL_ENABLED

Jenis Sumber Daya: AWS::OpenSearch::Domain

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

opensearch-audit-logging-enabled

Memeriksa apakah domain OpenSearch Layanan Amazon mengaktifkan pencatatan audit. Aturannya adalah NON_COMPLIANT jika domain OpenSearch Service tidak mengaktifkan audit logging.

Pengidentifikasi: OPENSEARCH_AUDIT_LOGGING_ENABLED

Jenis Sumber Daya: AWS::OpenSearch::Domain

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

cloudWatchLogsLogGroupArnList (Opsional), Jenis: CSV

> Daftar Nama Sumber Daya Amazon (ARNs) yang dipisahkan koma untuk grup CloudWatch log Amazon Logs. Aturan memeriksa apakah grup log yang ditentukan dikonfigurasi untuk log audit.
>
> Nilai yang valid meliputi: `arn:aws:logs:region:account-id:log-group:log_group_name:*` dan`arn:aws:logs:region:account-id:log-group:log_group_name`.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

opensearch-data-node-fault-toleransi

Memeriksa apakah domain OpenSearch Layanan Amazon dikonfigurasi dengan setidaknya tiga node data dan zoneAwarenessEnabled benar. Aturannya adalah NON_COMPLIANT untuk OpenSearch domain jika 'InstanceCount' kurang dari 3 atau '' disetel ke 'false'. zoneAwarenessEnabled

Pengidentifikasi: OPENSEARCH_DATA_NODE_FAULT_TOLERANCE

Jenis Sumber Daya: AWS::OpenSearch::Domain

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

opensearch-encrypted-at-rest

Memeriksa apakah domain OpenSearch Layanan Amazon mengaktifkan enkripsi saat konfigurasi istirahat. Aturannya adalah NON_COMPLIANT jika `EncryptionAtRestOptions` bidang tidak diaktifkan.

> **Note**
>
> Aturan tidak mengevaluasi domain Elasticsearch.

Pengidentifikasi: OPENSEARCH_ENCRYPTED_AT_REST

Jenis Sumber Daya: AWS::OpenSearch::Domain

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel

Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

opensearch-https-required

Memeriksa apakah koneksi ke OpenSearch domain menggunakan HTTPS. Aturannya adalah NON_COMPLIANT jika domain Amazon OpenSearch 'enforceHttps' tidak 'true' atau 'true' dan 'Policy' tidak ada di' '. TLSSecurity `tlsPolicies`

Pengidentifikasi: OPENSEARCH_HTTPS_REQUIRED

Jenis Sumber Daya: AWS::OpenSearch::Domain

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

TLSPolicies (Opsional), Jenis: CSV

> Daftar kebijakan keamanan TLS yang dipisahkan koma untuk memeriksa domain Amazon. OpensSearch

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

opensearch-in-vpc-only

Memeriksa apakah domain OpenSearch Layanan Amazon berada di Amazon Virtual Private Cloud (VPC). Aturannya adalah NON_COMPLIANT jika titik akhir domain OpenSearch Layanan bersifat publik.

> **Note**
>
> Aturan tidak mengevaluasi domain Elasticsearch.

Pengidentifikasi: OPENSEARCH_IN_VPC_ONLY

Jenis Sumber Daya: AWS::OpenSearch::Domain

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

opensearch-logs-to-cloudwatch

Memeriksa apakah domain OpenSearch Layanan Amazon dikonfigurasi untuk mengirim log ke CloudWatch Log Amazon. Aturannya adalah NON_COMPLIANT jika logging tidak dikonfigurasi.

> **Note**
>
> Aturan tidak mengevaluasi domain Elasticsearch.

Pengidentifikasi: OPENSEARCH_LOGS_TO_CLOUDWATCH

Jenis Sumber Daya: AWS::OpenSearch::Domain

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

LogTypes (Opsional), Jenis: CSV

> Daftar log yang dipisahkan koma yang diaktifkan. Nilai yang valid adalah 'pencarian', 'indeks', 'kesalahan'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

opensearch-node-to-node-pemeriksaan enkripsi-

Periksa apakah node OpenSearch Layanan Amazon dienkripsi ujung ke ujung. Aturannya adalah NON_COMPLIANT jika node-to-node enkripsi tidak diaktifkan pada domain

> **Note**
>
> Aturan tidak mengevaluasi domain Elasticsearch.

Pengidentifikasi: OPENSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

Jenis Sumber Daya: AWS::OpenSearch::Domain

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

opensearch-primary-node-fault-toleransi

Memeriksa apakah domain OpenSearch Layanan Amazon dikonfigurasi dengan setidaknya tiga node utama khusus. Aturannya adalah NON_COMPLIANT untuk domain OpenSearch Layanan jika 'DedicatedMasterEnabled' disetel ke 'false', atau 'DedicatedMasterCount' kurang dari 3.

Pengidentifikasi: OPENSEARCH_PRIMARY_NODE_FAULT_TOLERANCE

Jenis Sumber Daya: AWS::OpenSearch::Domain

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Eropa (Ningxia), Eropa Wilayah (Zurich)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

opensearch-update-check

Memeriksa apakah pembaruan versi OpenSearch Layanan Amazon tersedia tetapi tidak diinstal. Aturannya adalah NON_COMPLIANT untuk OpenSearch domain jika pembaruan perangkat lunak terbaru tidak diinstal.

Pengidentifikasi: OPENSEARCH_UPDATE_CHECK

Jenis Sumber Daya: AWS::OpenSearch::Domain

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

rabbit-mq-supported-version

Memeriksa apakah broker Amazon MQ RabbitMQ berjalan pada versi mesin minimum yang didukung. Aturannya adalah NON_COMPLIANT jika broker RabbitMQ tidak berjalan pada versi mesin minimum yang didukung yang Anda tentukan.

Pengidentifikasi: RABBIT_MQ_SUPPORTED_VERSION

Jenis Sumber Daya: AWS::AmazonMQ::Broker

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

supportedEngineVersion, Tipe: String

Nilai string untuk aturan untuk memeriksa versi mesin minimum yang didukung untuk broker RabbitMQ. Broker RabbitMQ menggunakan spesifikasi versi semantik: XYZ X menunjukkan versi utama, Y mewakili versi minor, dan Z menunjukkan versi patch.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

rds-aurora-mysql-audit-logging-diaktifkan

Memeriksa apakah klaster Edisi yang kompatibel dengan Amazon Aurora MySQL dikonfigurasi untuk mempublikasikan log audit ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika klaster Edisi yang kompatibel dengan Aurora MySQL tidak memiliki publikasi log audit yang dikonfigurasi.

Pengidentifikasi: RDS_AURORA_MYSQL_AUDIT_LOGGING_ENABLED

Jenis Sumber Daya: AWS::RDS::DBCluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary) Wilayah

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

rds-aurora-postgresql-logske cloudwatch

Memeriksa apakah klaster DB PostgreSQL Amazon Aurora dikonfigurasi untuk mempublikasikan log PostgreSQL ke Amazon Logs. CloudWatch Aturan ini NON_COMPLIANT jika cluster DB tidak dikonfigurasi untuk mempublikasikan log PostgreSQL ke Amazon Logs. CloudWatch

Pengidentifikasi: RDS_AURORA_POSTGRESQL_LOGS_TO_CLOUDWATCH

Jenis Sumber Daya: AWS::RDS::DBCluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Eropa (Spanyol)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

rds-automatic-minor-version-upgrade diaktifkan

Memeriksa apakah instans database Amazon Relational Database Service (Amazon RDS) dikonfigurasi untuk upgrade versi minor otomatis. Aturannya adalah NON_COMPLIANT jika nilai 'autoMinorVersionUpgrade' salah.

Pengidentifikasi: RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED

Jenis Sumber Daya: AWS::RDS::DBInstance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

Tidak ada

Evaluasi Proaktif

Untuk langkah-langkah tentang cara menjalankan aturan ini dalam mode proaktif, lihat Mengevaluasi Sumber Daya Anda dengan AWS Config Aturan. Agar aturan ini mengembalikan COMPLIANT dalam mode proaktif, skema konfigurasi sumber daya untuk StartResourceEvaluationAPI harus menyertakan input berikut, yang dikodekan sebagai string:

```
"ResourceConfiguration":
...
{
    "AutoMinorVersionUpgrade": BOOLEAN*,
    "Engine": String*
}
...
```

* Untuk informasi lebih lanjut tentang nilai yang valid untuk input ini, lihat AutoMinorVersionUpgrade dan Mesin di Panduan AWS CloudFormation Pengguna.

Untuk informasi lebih lanjut tentang evaluasi proaktif, lihat Mode Evaluasi.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

rds-cluster-auto-minor-version-upgrade-enable

Memeriksa apakah upgrade versi minor otomatis diaktifkan untuk penerapan klaster Amazon RDS Multi-AZ. Aturannya adalah NON_COMPLIANT jika autoMinorVersion Upgrade disetel ke false.

Pengidentifikasi: RDS_CLUSTER_AUTO_MINOR_VERSION_UPGRADE_ENABLE

Jenis Sumber Daya: AWS::RDS::DBCluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), AS Barat (California N.), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

rds-cluster-default-admin-periksa

Memeriksa apakah kluster database Amazon Relational Database Service (Amazon RDS) telah mengubah nama pengguna admin dari nilai defaultnya. Aturannya adalah NON_COMPLIANT jika nama pengguna admin disetel ke nilai default.

Pengidentifikasi: RDS_CLUSTER_DEFAULT_ADMIN_CHECK

Jenis Sumber Daya: AWS::RDS::DBCluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Tiongkok (Ningxia) Wilayah

Parameter:

validAdminUserNama (Opsional), Jenis: CSV

> Daftar nama pengguna admin yang dipisahkan koma yang dapat digunakan kluster Amazon RDS. Tidak dapat menyertakan 'postgres' atau 'admin' sebagai nama pengguna yang valid karena ini adalah nilai default.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

rds-cluster-deletion-protection-diaktifkan

Memeriksa apakah klaster Amazon Relational Database Service (Amazon RDS) telah mengaktifkan perlindungan penghapusan. Aturannya adalah NON_COMPLIANT jika klaster Amazon RDS tidak mengaktifkan perlindungan penghapusan.

Pengidentifikasi: RDS_CLUSTER_DELETION_PROTECTION_ENABLED

Jenis Sumber Daya: AWS::RDS::DBCluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Tiongkok (Beijing)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

rds-cluster-encrypted-at-istirahat

Memeriksa apakah kluster Amazon Relational Database Service (Amazon RDS) dienkripsi saat istirahat. Aturannya adalah NON_COMPLIANT jika klaster Amazon RDS tidak dienkripsi saat istirahat.

Pengidentifikasi: RDS_CLUSTER_ENCRYPTED_AT_REST

Jenis Sumber Daya: AWS::RDS::DBCluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia) AWS GovCloud , (AS-Timur), (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

rds-cluster-iam-authentication-diaktifkan

Memeriksa apakah klaster AWS Amazon Relational Database Service (Amazon RDS) mengaktifkan autentikasi Identity and Access Management (IAM). Aturannya adalah NON_COMPLIANT jika Cluster Amazon RDS tidak mengaktifkan autentikasi IAM.

Pengidentifikasi: RDS_CLUSTER_IAM_AUTHENTICATION_ENABLED

Jenis Sumber Daya: AWS::RDS::DBCluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Tiongkok (Beijing)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

rds-cluster-multi-az-diaktifkan

Memeriksa apakah replikasi Multi-Availability Zone (Multi-AZ) diaktifkan di Amazon Aurora dan cluster DB Multi-AZ yang dikelola oleh Amazon Relational Database Service (Amazon RDS). Aturannya adalah NON_COMPLIANT jika instans Amazon RDS tidak dikonfigurasi dengan Multi-AZ.

Pengidentifikasi: RDS_CLUSTER_MULTI_AZ_ENABLED

Jenis Sumber Daya: AWS::RDS::DBCluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Wilayah Asia Pasifik (Melbourne)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

rds-db-security-group-tidak diizinkan

Memeriksa apakah ada grup keamanan DB Amazon Relational Database Service (Amazon RDS) yang bukan grup keamanan DB default. Aturannya adalah NON_COMPLIANT jika ada grup keamanan DB yang bukan grup keamanan DB default.

Pengidentifikasi: RDS_DB_SECURITY_GROUP_NOT_ALLOWED

Jenis Sumber Daya: AWS::RDS::DBSecurityGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Eropa (Irlandia), Amerika Selatan (Sao Paulo), AS Timur (Virginia N.), Asia Pasifik (Tokyo), AS Barat (Oregon), AS Barat (California N.), Asia Pasifik (Singapura), Wilayah Asia Pasifik (Sydney)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

rds-enhanced-monitoring-enabled

Memeriksa apakah pemantauan yang disempurnakan diaktifkan untuk instans Amazon RDS. Aturan ini adalah NON_COMPLIANT jika `monitoringInterval` " adalah '0' dalam item konfigurasi instance RDS, atau jika '`monitoringInterval`' tidak cocok dengan nilai parameter aturan.

Pengidentifikasi: RDS_ENHANCED_MONITORING_ENABLED

Jenis Sumber Daya: AWS::RDS::DBInstance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

MonitoringInterval (Opsional), Jenis: int

Nilai integer dalam hitungan detik antar titik saat metrik pemantauan yang ditingkatkan dikumpulkan untuk instance database. Nilai yang valid adalah 1, 5, 10, 15, 30, dan 60.

Evaluasi Proaktif

Untuk langkah-langkah tentang cara menjalankan aturan ini dalam mode proaktif, lihat Mengevaluasi Sumber Daya Anda dengan AWS Config Aturan. Agar aturan ini mengembalikan COMPLIANT dalam mode proaktif, skema konfigurasi sumber daya untuk StartResourceEvaluationAPI harus menyertakan input berikut, yang dikodekan sebagai string:

```
"ResourceConfiguration":
...
{
    "MonitoringInterval": Integer*,
    "Engine": String*
}
...
```

* Untuk informasi lebih lanjut tentang nilai yang valid untuk input ini, lihat MonitoringIntervaldan Mesin di Panduan AWS CloudFormation Pengguna.

Untuk informasi lebih lanjut tentang evaluasi proaktif, lihat Mode Evaluasi.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

rds-instance-default-admin-periksa

Memeriksa apakah database Amazon Relational Database Service (Amazon RDS) telah mengubah nama pengguna admin dari nilai defaultnya. Aturan ini hanya akan berjalan pada instance database RDS. Aturannya adalah NON_COMPLIANT jika nama pengguna admin disetel ke nilai default.

Pengidentifikasi: RDS_INSTANCE_DEFAULT_ADMIN_CHECK

Jenis Sumber Daya: AWS::RDS::DBInstance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

validAdminUserNama (Opsional), Jenis: CSV

> Daftar nama pengguna admin yang dipisahkan koma yang dapat digunakan instans Amazon RDS. (Tidak dapat menyertakan 'postgres' atau 'admin' sebagai nama pengguna yang valid karena ini adalah nilai default.)

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

rds-instance-deletion-protection-diaktifkan

Memeriksa apakah instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Aturannya adalah NON_COMPLIANT jika instance Amazon RDS tidak mengaktifkan perlindungan penghapusan; misalnya, DeletionProtection disetel ke false.

> **Warning**
>
> Beberapa instans RDS DB dalam Cluster (Aurora/DocumentDB) akan ditampilkan sebagai tidak sesuai.

Pengidentifikasi: RDS_INSTANCE_DELETION_PROTECTION_ENABLED

Jenis Sumber Daya: AWS::RDS::DBInstance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

DatabaseEngines (Opsional), Jenis: CSV

Daftar mesin database RDS yang dipisahkan koma untuk dimasukkan dalam evaluasi aturan. Misalnya, 'mysql, postgres, mariadb'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

rds-instance-iam-authentication-diaktifkan

Memeriksa apakah instans AWS Amazon Relational Database Service (Amazon RDS) mengaktifkan autentikasi Identity and Access Management (IAM). Aturannya adalah NON_COMPLIANT jika instans Amazon RDS tidak mengaktifkan autentikasi IAM.

> **Note**
>
> Mesin DB harus menjadi salah satu dari 'mysql', 'postgres', 'aurora', 'aurora-mysql', atau 'aurora-postgresql'. Status instans DB harus menjadi salah satu dari 'tersedia', 'backing-up', 'storage-optimization', atau 'storage-full'.

Pengidentifikasi: RDS_INSTANCE_IAM_AUTHENTICATION_ENABLED

Jenis Sumber Daya: AWS::RDS::DBInstance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

rds-instance-public-access-periksa

Memeriksa apakah instans Amazon Relational Database Service (Amazon RDS) tidak dapat diakses publik. Aturannya adalah NON_COMPLIANT jika bidang PubliclyAccessible benar dalam item konfigurasi instance.

Pengidentifikasi: RDS_INSTANCE_PUBLIC_ACCESS_CHECK

Jenis Sumber Daya: AWS::RDS::DBInstance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

Tidak ada

Evaluasi Proaktif

Untuk langkah-langkah tentang cara menjalankan aturan ini dalam mode proaktif, lihat Mengevaluasi Sumber Daya Anda dengan AWS Config Aturan. Agar aturan ini mengembalikan COMPLIANT dalam mode proaktif, skema konfigurasi sumber daya untuk StartResourceEvaluationAPI harus menyertakan input berikut, yang dikodekan sebagai string:

```
"ResourceConfiguration":
...
{
   "PubliclyAccessible": BOOLEAN
}
...
```

Untuk informasi lebih lanjut tentang evaluasi proaktif, lihat Mode Evaluasi.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

rds-instance-subnet-igw-periksa

Memeriksa apakah instans RDS DB digunakan di subnet publik dengan rute ke gateway internet. Aturannya adalah NON_COMPLIANT jika instance RDS DB diterapkan di subnet publik

Pengidentifikasi: RDS_INSTANCE_SUBNET_IGW_CHECK

Jenis Sumber Daya: AWS::RDS::DBInstance

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (Bahrain), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

rds-in-backup-plan

Memeriksa apakah database Amazon Relational Database Service (Amazon RDS) ada dalam AWS paket Backup. Aturannya adalah NON_COMPLIANT jika database Amazon RDS tidak disertakan dalam paket Backup apa pun. AWS

> **Note**
>
> Aturan ini hanya berlaku untuk instans Amazon Aurora DB. Cluster DB tidak didukung.

Pengidentifikasi: RDS_IN_BACKUP_PLAN

Jenis Sumber Daya: AWS::RDS::DBInstance

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei), Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

rds-last-backup-recovery-point-dibuat

Memeriksa apakah titik pemulihan dibuat untuk Amazon Relational Database Service (Amazon RDS). Aturannya adalah NON_COMPLIANT jika instans Amazon RDS tidak memiliki titik pemulihan terkait yang dibuat dalam periode waktu yang ditentukan.

Pengidentifikasi: RDS_LAST_BACKUP_RECOVERY_POINT_CREATED

Jenis Sumber Daya: AWS::RDS::DBInstance

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

ResourceTags (Opsional), Tipe: String

Tag instans Amazon RDS untuk aturan yang akan diperiksa, dalam format JSON. `{"tagkey" : "tagValue"}`

ResourceID (Opsional), Tipe: String

ID instans Amazon RDS untuk aturan yang akan diperiksa.

recoveryPointAgeNilai (Opsional), Jenis: int, Default: 1

Nilai numerik untuk usia maksimum yang diizinkan. Tidak lebih dari 744 jam, 31 untuk hari.

recoveryPointAgeUnit (Opsional), Tipe: String, Default: hari

Satuan waktu untuk usia maksimum yang diizinkan. Nilai yang diterima: 'jam', 'hari'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

rds-logging-enabled

Memeriksa apakah log masing-masing Amazon Relational Database Service (Amazon RDS) diaktifkan. Aturannya adalah NON_COMPLIANT jika ada jenis log yang tidak diaktifkan.

> **Note**
>
> Instans DB yang tidak ada dalam status 'tersedia', 'cadangan', 'optimasi penyimpanan', atau 'penuh-penyimpanan' dievaluasi sebagai. `NOT_APPLICABLE`

Pengidentifikasi: RDS_LOGGING_ENABLED

Jenis Sumber Daya: AWS::RDS::DBInstance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

AdditionalLogs (Opsional), Jenis: StringMap

Daftar nama mesin dan nama jenis log yang dipisahkan koma. Misalnya, “additionalLogs”: “oracle: general, slowquery; aurora: alert, slowquery”

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

rds-mariadb-instance-encrypted-dalam transit

Memeriksa apakah koneksi ke Amazon RDS untuk instans DB MariaDB dengan versi engine lebih besar dari atau sama dengan 10,5 menggunakan enkripsi dalam perjalanan. Aturannya adalah NON_COMPLIANT jika grup parameter DB tidak sinkron atau jika require_secure_transport tidak disetel ke ON.

Pengidentifikasi: RDS_MARIADB_INSTANCE_ENCRYPTED_IN_TRANSIT

Jenis Sumber Daya: AWS::RDS::DBInstance

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (Bahrain), Tiongkok (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

rds-meets-restore-time-target

Memeriksa apakah waktu pemulihan instans Amazon Relational Database Service (Amazon RDS) memenuhi durasi yang ditentukan. Aturannya adalah NON_COMPLIANT jika LatestRestoreExecutionTimeMinutes instans Amazon RDS lebih besar dari menit. maxRestoreTime

Pengidentifikasi: RDS_MEETS_RESTORE_TIME_TARGET

Jenis Sumber Daya: AWS::RDS::DBInstance

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

maxRestoreTime, Jenis: int

Nilai numerik untuk runtime pemulihan maksimum yang diizinkan.

ResourceTags (Opsional), Tipe: String

Tag instans Amazon RDS untuk aturan yang akan diperiksa, dalam format JSON.

ResourceID (Opsional), Tipe: String

ID instans Amazon RDS untuk aturan yang akan diperiksa.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

rds-multi-az-support

Memeriksa apakah ketersediaan tinggi diaktifkan untuk instans RDS DB Anda.

Dalam penerapan Multi-AZ, Amazon RDS secara otomatis menyediakan dan mempertahankan replika siaga yang sinkron di Availability Zone yang berbeda. Untuk informasi selengkapnya, lihat Ketersediaan Tinggi (Multi-AZ) di Panduan Pengguna Amazon RDS.

> **Note**
>
> Aturan ini tidak mengevaluasi instans Amazon Aurora DB, Amazon DocumentDB, dan Amazon Neptune DB.

Pengidentifikasi: RDS_MULTI_AZ_SUPPORT

Jenis Sumber Daya: AWS::RDS::DBInstance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

Tidak ada

Evaluasi Proaktif

Untuk langkah-langkah tentang cara menjalankan aturan ini dalam mode proaktif, lihat Mengevaluasi Sumber Daya Anda dengan AWS Config Aturan. Agar aturan ini mengembalikan COMPLIANT dalam mode proaktif, skema konfigurasi sumber daya untuk StartResourceEvaluationAPI harus menyertakan input berikut, yang dikodekan sebagai string:

```
"ResourceConfiguration":
...
{
    "MultiAZ": BOOLEAN*,
    "Engine": String*
}
...
```

* Untuk informasi selengkapnya tentang nilai valid untuk input ini, lihat MultiAZ dan Engine di Panduan Pengguna AWS CloudFormation .

Untuk informasi lebih lanjut tentang evaluasi proaktif, lihat Mode Evaluasi.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

rds-mysql-instance-encrypted-dalam transit

Memeriksa apakah koneksi ke Amazon RDS untuk instance database MySQL dikonfigurasi untuk menggunakan enkripsi dalam perjalanan. Aturannya adalah NON_COMPLIANT jika grup parameter database terkait tidak sinkron atau jika parameter require_secure_transport tidak disetel ke 1.

> **Note**
>
> Aturan kembali `NOT_APPLICABLE` jika instans Amazon RDS adalah bagian dari cluster RDS.

Pengidentifikasi: RDS_MYSQL_INSTANCE_ENCRYPTED_IN_TRANSIT

Jenis Sumber Daya: AWS::RDS::DBInstance

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

rds-postgresql-logs-to-jam tangan awan

Memeriksa apakah instans Amazon PostgreSQL DB dikonfigurasi untuk mempublikasikan log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika instans DB tidak dikonfigurasi untuk mempublikasikan log ke Amazon Logs. CloudWatch

Pengidentifikasi: RDS_POSTGRESQL_LOGS_TO_CLOUDWATCH

Jenis Sumber Daya: AWS::RDS::DBInstance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

LogTypes (Opsional), Jenis: CSV

> Daftar tipe log yang dipisahkan koma untuk dipublikasikan ke CloudWatch Log. Nilai yang valid adalah: 'postgresql', 'upgrade'. Nilai default adalah 'postgresql'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

rds-postgres-instance-encrypted-dalam transit

Memeriksa apakah koneksi ke instance database Amazon RDS PostgreSQL dikonfigurasi untuk menggunakan enkripsi saat transit. Aturannya adalah NON_COMPLIANT jika grup parameter database terkait tidak sinkron atau jika parameter rds.force_ssl tidak disetel ke 1.

> **Note**
>
> Aturan kembali `NOT_APPLICABLE` jika instans Amazon RDS adalah bagian dari cluster RDS.

Pengidentifikasi: RDS_POSTGRES_INSTANCE_ENCRYPTED_IN_TRANSIT

Jenis Sumber Daya: AWS::RDS::DBInstance

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

rds-proxy-tls-encryption

Memeriksa apakah proxy Amazon RDS memberlakukan TLS untuk semua koneksi. Aturannya adalah NON_COMPLIANT jika proxy Amazon RDS tidak menerapkan TLS untuk semua koneksi.

Pengidentifikasi: RDS_PROXY_TLS_ENCRYPTION

Jenis Sumber Daya: AWS::RDS::DBProxy

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (Bahrain), Tiongkok (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur), AWS GovCloud (AS-Barat),

Meksiko AWS GovCloud (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

rds-resources-protected-by-rencana cadangan

Memeriksa apakah instans Amazon Relational Database Service (Amazon RDS) dilindungi oleh paket cadangan. Aturannya adalah NON_COMPLIANT jika instans Amazon RDS Database tidak dicakup oleh paket cadangan.

Pengidentifikasi: RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Jenis Sumber Daya: AWS::RDS::DBInstance

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

ResourceTags (Opsional), Tipe: String

Tag untuk instans Amazon RDS untuk aturan yang akan diperiksa, dalam format JSON. `{"tagkey" : "tagValue"}`

ResourceID (Opsional), Tipe: String

ID instans Amazon RDS untuk aturan yang akan diperiksa.

crossRegionList (Opsional), Tipe: String

Daftar wilayah tujuan yang dipisahkan koma untuk salinan cadangan lintas wilayah yang akan disimpan

crossAccountList (Opsional), Tipe: String

Daftar akun tujuan yang dipisahkan koma untuk salinan cadangan lintas akun yang akan disimpan

maxRetentionDays (Opsional), Jenis: int

Periode retensi maksimum dalam beberapa hari untuk Backup Vault Lock

minRetentionDays (Opsional), Jenis: int

Periode retensi minimum dalam beberapa hari untuk Backup Vault Lock

backupVaultLockPeriksa (Opsional), Tipe: String

Nilai yang diterima: 'Benar' atau 'False'. Masukkan 'Benar' untuk aturan untuk memeriksa apakah sumber daya dicadangkan di brankas yang terkunci

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

rds-snapshots-public-prohibited

Memeriksa apakah snapshot Amazon Relational Database Service (Amazon RDS) bersifat publik. Aturannya adalah NON_COMPLIANT jika ada snapshot Amazon RDS yang ada dan yang baru bersifat publik.

> **Note**
>
> Diperlukan waktu hingga 12 jam untuk menangkap hasil kepatuhan.

Pengidentifikasi: RDS_SNAPSHOTS_PUBLIC_FORBIDLED

Jenis Sumber Daya: AWS::RDS::DBSnapshot, AWS::RDS::DBClusterSnapshot

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Afrika (Cape Town), Asia Pasifik (Melbourne), Eropa (Milan), Israel (Tel Aviv), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

rds-snapshot-encrypted

Memeriksa apakah snapshot DB Amazon Relational Database Service (Amazon RDS) dienkripsi. Aturannya adalah NON_COMPLIANT jika snapshot Amazon RDS DB tidak dienkripsi.

Pengidentifikasi: RDS_SNAPSHOT_ENCRYPTED

Jenis Sumber Daya: AWS::RDS::DBSnapshot, AWS::RDS::DBClusterSnapshot

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

rds-sqlserver-encrypted-in-transit

Memeriksa apakah koneksi ke instans database server Amazon RDS SQL dikonfigurasi untuk menggunakan enkripsi dalam perjalanan. Aturannya adalah NON_COMPLIANT jika parameter DB force_ssl untuk grup parameter tidak disetel ke 1 atau parameternya bukan 'in-sync'. ApplyStatus

Pengidentifikasi: RDS_SQLSERVER_ENCRYPTED_IN_TRANSIT

Jenis Sumber Daya: AWS::RDS::DBInstance

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (Bahrain), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

rds-sql-server-logske cloudwatch

Memeriksa apakah instans Amazon SQL Server DB dikonfigurasi untuk mempublikasikan log ke Amazon CloudWatch Logs. Aturan ini NON_COMPLIANT jika instans DB tidak dikonfigurasi untuk mempublikasikan log ke Amazon Logs. CloudWatch

Pengidentifikasi: RDS_SQL_SERVER_LOGS_TO_CLOUDWATCH

Jenis Sumber Daya: AWS::RDS::DBInstance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

LogTypes (Opsional), Jenis: CSV

> LogTypes - (Opsional): Daftar tipe log yang dipisahkan koma untuk dipublikasikan ke Log. CloudWatch Nilai yang valid adalah: 'error', 'agen'. Nilai default adalah 'kesalahan', 'agen'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

rds-storage-encrypted

Memeriksa apakah enkripsi penyimpanan diaktifkan untuk instans DB Amazon Relational Database Service (Amazon RDS) Anda. Aturannya adalah NON_COMPLIANT jika enkripsi penyimpanan tidak diaktifkan.

Pengidentifikasi: RDS_STORAGE_ENCRYPTED

Jenis Sumber Daya: AWS::RDS::DBInstance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

kmsKeyId (Opsional), Tipe: String

> ID kunci KMS atau Nama Sumber Daya Amazon (ARN) digunakan untuk mengenkripsi penyimpanan.

Evaluasi Proaktif

Untuk langkah-langkah tentang cara menjalankan aturan ini dalam mode proaktif, lihat Mengevaluasi Sumber Daya Anda dengan AWS Config Aturan. Agar aturan ini mengembalikan COMPLIANT dalam mode proaktif, skema konfigurasi sumber daya untuk StartResourceEvaluationAPI harus menyertakan input berikut, yang dikodekan sebagai string:

```
"ResourceConfiguration":
...
{
   "StorageEncrypted": BOOLEAN
}
...
```

Untuk informasi lebih lanjut tentang evaluasi proaktif, lihat Mode Evaluasi.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

redshift-audit-logging-enabled

Memeriksa apakah klaster Amazon Redshift mencatat audit ke bucket tertentu. Aturannya adalah NON_COMPLIANT jika pencatatan audit tidak diaktifkan untuk klaster Redshift atau jika parameter '`bucketNames`' disediakan tetapi tujuan pencatatan audit tidak cocok.

Pengidentifikasi: REDSHIFT_AUDIT_LOGGING_ENABLED

Jenis Sumber Daya: AWS::Redshift::Cluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

BucketNames (Opsional), Jenis: CSV

Daftar nama bucket Amazon S3 yang dipisahkan koma untuk menyimpan log audit.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

redshift-backup-enabled

Memeriksa apakah snapshot otomatis Amazon Redshift diaktifkan untuk cluster. Aturannya adalah NON_COMPLIANT jika nilai untuk `automatedSnapshotRetentionPeriod` lebih besar dari `MaxRetentionPeriod` atau kurang dari `MinRetentionPeriod` atau nilainya 0.

Pengidentifikasi: REDSHIFT_BACKUP_ENABLED

Jenis Sumber Daya: AWS::Redshift::Cluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

MinRetentionPeriod (Opsional), Jenis: int

Nilai minimum untuk periode retensi. Nilai minimum adalah 1.

MaxRetentionPeriod (Opsional), Jenis: int

Nilai maksimum untuk periode retensi. Nilai maksimum adalah 35.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

redshift-cluster-configuration-check

Memeriksa apakah cluster Amazon Redshift memiliki pengaturan yang ditentukan. Aturannya adalah NON_COMPLIANT jika klaster Amazon Redshift tidak dienkripsi atau dienkripsi dengan kunci lain, atau jika klaster tidak mengaktifkan pencatatan audit.

Pengidentifikasi: REDSHIFT_CLUSTER_CONFIGURATION_CHECK

Jenis Sumber Daya: AWS::Redshift::Cluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol) Wilayah

Parameter:

clusterDbEncrypted, Jenis: boolean, Default: betul

Enkripsi basis data diaktifkan.

loggingEnabled, Jenis: boolean, Default: betul

Pencatatan audit diaktifkan.

NodeTypes (Opsional), Jenis: CSV, Default: dc1.large

Tentukan jenis simpul.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

redshift-cluster-kms-enabled

Memeriksa apakah klaster Amazon Redshift menggunakan kunci AWS Key Management Service (AWS KMS) tertentu untuk enkripsi. Aturannya adalah COMPLIANT jika enkripsi diaktifkan dan cluster dienkripsi dengan kunci yang disediakan dalam parameter. `kmsKeyArn` Aturannya adalah NON_COMPLIANT jika cluster tidak dienkripsi atau dienkripsi dengan kunci lain.

Pengidentifikasi: REDSHIFT_CLUSTER_KMS_ENABLED

Jenis Sumber Daya: AWS::Redshift::Cluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Meksiko (Tengah), Wilayah Asia Pasifik (Taipei)

Parameter:

kmsKeyArns (Opsional), Jenis: CSV

> Daftar Nama Sumber Daya AWS KMS Amazon (ARNs) yang dipisahkan koma yang digunakan dalam klaster Amazon Redshift untuk enkripsi.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

redshift-cluster-maintenancesettings-check

Memeriksa apakah klaster Amazon Redshift memiliki pengaturan pemeliharaan yang ditentukan. Aturannya adalah NON_COMPLIANT jika upgrade otomatis ke versi mayor dinonaktifkan.

Pengidentifikasi: REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK

Jenis Sumber Daya: AWS::Redshift::Cluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Meksiko (Tengah), Wilayah Asia Pasifik (Taipei)

Parameter:

allowVersionUpgrade, Jenis: boolean, Default: betul

Izinkan peningkatan versi diaktifkan.

preferredMaintenanceWindow (Opsional), Tipe: String

Jendela pemeliharaan terjadwal untuk cluster (misalnya, Senin: 09:30 -Senin: 10:00).

automatedSnapshotRetentionPeriode (Opsional), Jenis: int, Default: 1

Jumlah hari untuk menyimpan snapshot otomatis.

Evaluasi Proaktif

Untuk langkah-langkah tentang cara menjalankan aturan ini dalam mode proaktif, lihat Mengevaluasi Sumber Daya Anda dengan AWS Config Aturan. Agar aturan ini mengembalikan COMPLIANT dalam mode proaktif, skema konfigurasi sumber daya untuk StartResourceEvaluationAPI harus menyertakan input berikut, yang dikodekan sebagai string:

```
"ResourceConfiguration":
...
{
    "AutomatedSnapshotRetentionPeriod": Integer*,
    "PreferredMaintenanceWindow": String*,
    "AllowVersionUpgrade": BOOLEAN*
}
...
```

* Untuk informasi lebih lanjut tentang nilai yang valid untuk input ini, lihat AutomatedSnapshotRetentionPeriod, PreferredMaintenanceWindow, dan AllowVersionUpgradedi Panduan AWS CloudFormation Pengguna.

Untuk informasi lebih lanjut tentang evaluasi proaktif, lihat Mode Evaluasi.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

redshift-cluster-multi-az-diaktifkan

Memeriksa apakah klaster Amazon Redshift memiliki beberapa penerapan Availability Zones yang diaktifkan. Aturan ini NON_COMPLIANT jika klaster Amazon Redshift tidak mengaktifkan beberapa penerapan Availability Zones.

Pengidentifikasi: REDSHIFT_CLUSTER_MULTI_AZ_ENABLED

Jenis Sumber Daya: AWS::Redshift::Cluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Seoul), Asia Pasifik (Malaysia), Meksiko (Tengah), AS Barat (California N.), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

redshift-cluster-parameter-group-ditandai

Memeriksa apakah grup parameter klaster Amazon Redshift memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: REDSHIFT_CLUSTER_PARAMETER_GROUP_TAGGED

Jenis Sumber Daya: AWS::Redshift::ClusterParameterGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

redshift-cluster-public-access-periksa

Memeriksa apakah klaster Amazon Redshift tidak dapat diakses publik. Aturannya adalah NON_COMPLIANT jika bidang PubliclyAccessible adalah True di item konfigurasi cluster.

Pengidentifikasi: REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK

Jenis Sumber Daya: AWS::Redshift::Cluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Meksiko (Tengah), Wilayah Asia Pasifik (Taipei)

Parameter:

Tidak ada

Evaluasi Proaktif

Untuk langkah-langkah tentang cara menjalankan aturan ini dalam mode proaktif, lihat Mengevaluasi Sumber Daya Anda dengan AWS Config Aturan. Agar aturan ini mengembalikan COMPLIANT dalam mode proaktif, skema konfigurasi sumber daya untuk StartResourceEvaluationAPI harus menyertakan input berikut, yang dikodekan sebagai string:

```
"ResourceConfiguration":
...
{
```

```
   "PubliclyAccessible": BOOLEAN
}
...
```

Untuk informasi lebih lanjut tentang evaluasi proaktif, lihat Mode Evaluasi.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

redshift-cluster-subnet-group-multi-az

Memeriksa apakah grup subnet Amazon Redshift berisi subnet dari lebih dari satu Availability Zone. Aturannya adalah NON_COMPLIANT jika grup subnet Amazon Redshift tidak berisi subnet dari setidaknya dua Availability Zone yang berbeda.

Pengidentifikasi: REDSHIFT_CLUSTER_SUBNET_GROUP_MULTI_AZ

Jenis Sumber Daya: AWS::Redshift::ClusterSubnetGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

redshift-default-admin-check

Memeriksa apakah klaster Amazon Redshift telah mengubah nama pengguna admin dari nilai defaultnya. Aturannya adalah NON_COMPLIANT jika nama pengguna admin untuk klaster Redshift disetel ke “awsuser” atau jika nama pengguna tidak cocok dengan apa yang tercantum dalam parameter.

Pengidentifikasi: REDSHIFT_DEFAULT_ADMIN_CHECK

Jenis Sumber Daya: AWS::Redshift::Cluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

validAdminUserNama (Opsional), Jenis: CSV

Daftar nama pengguna admin yang dipisahkan koma untuk digunakan kluster Redshift. Catatan: 'awsuser' adalah default dan tidak diterima.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

redshift-default-db-name-periksa

Memeriksa apakah cluster Redshift telah mengubah nama database-nya dari nilai default. Aturannya adalah NON_COMPLIANT jika nama database untuk cluster Redshift disetel ke “dev”, atau jika parameter opsional disediakan dan nama database tidak cocok.

Pengidentifikasi: REDSHIFT_DEFAULT_DB_NAME_CHECK

Jenis Sumber Daya: AWS::Redshift::Cluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur), AWS GovCloud AWS GovCloud (AS-Barat), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

validDatabaseNames (Opsional), Jenis: CSV

Daftar nama database yang dipisahkan koma untuk kluster Redshift.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

redshift-enhanced-vpc-routing-diaktifkan

Memeriksa apakah klaster Amazon Redshift telah enhancedVpcRouting 'diaktifkan. Aturannya adalah NON_COMPLIANT jika 'enhancedVpcRouting' tidak diaktifkan atau jika konfigurasi. enhancedVpcRouting lapangan adalah 'palsu'.

Pengidentifikasi: REDSHIFT_ENHANCED_VPC_ROUTING_ENABLED

Jenis Sumber Daya: AWS::Redshift::Cluster

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Meksiko (Tengah), Wilayah Asia Pasifik (Taipei)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

redshift-require-tls-ssl

Memeriksa apakah klaster Amazon Redshift memerlukan TLS/SSL enkripsi untuk terhubung ke klien SQL. Aturannya adalah NON_COMPLIANT jika ada klaster Amazon Redshift yang memiliki parameter Require_SSL yang tidak disetel ke true.

Pengidentifikasi: REDSHIFT_REQUIRE_TLS_SSL

Jenis Sumber Daya: AWS::Redshift::Cluster, AWS::Redshift::ClusterParameterGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Meksiko (Tengah), Wilayah Asia Pasifik (Taipei)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

redshift-serverless-default-admin-periksa

Memeriksa apakah Namespace Tanpa Server Amazon Redshift telah mengubah nama pengguna admin dari nilai defaultnya. Aturannya adalah NON_COMPLIANT jika nama pengguna admin untuk Redshift Serverless Namespace disetel ke “admin”.

Pengidentifikasi: REDSHIFT_SERVERLESS_DEFAULT_ADMIN_CHECK

Jenis Sumber Daya: AWS::RedshiftServerless::Namespace

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (Bahrain), Asia Pasifik (Thailand), Afrika (Cape Town), Asia Pasifik (Hyderabad), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Eropa (Milan), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

redshift-serverless-default-db-nama-cek

Memeriksa apakah namespace Amazon Redshift Tanpa Server telah mengubah nama database-nya dari nilai default. Aturannya adalah NON_COMPLIANT jika nama database untuk namespace Amazon Redshift Tanpa Server disetel ke `dev`.

Pengidentifikasi: REDSHIFT_SERVERLESS_DEFAULT_DB_NAME_CHECK

Jenis Sumber Daya: AWS::RedshiftServerless::Namespace

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (Bahrain), Asia Pasifik (Thailand), Afrika (Cape Town), Asia Pasifik (Hyderabad), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Eropa (Milan), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

redshift-serverless-namespace-cmk-enkripsi

Memeriksa apakah ruang nama Amazon Redshift Tanpa Server dienkripsi oleh kunci KMS yang dikelola pelanggan. AWS Aturannya adalah NON_COMPLIANT jika namespace tidak dienkripsi oleh kunci yang dikelola pelanggan. Secara opsional, Anda dapat menentukan daftar kunci KMS untuk aturan untuk diperiksa.

Pengidentifikasi: REDSHIFT_SERVERLESS_NAMESPACE_CMK_ENCRYPTION

Jenis Sumber Daya: AWS::RedshiftServerless::Namespace

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (Bahrain), Asia Pasifik (Thailand), Afrika (Cape Town), Asia Pasifik (Hyderabad), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Eropa (Milan), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

kmsKeyArns (Opsional), Jenis: CSV

Daftar Amazon Resource Names (ARNs) kunci terkelola pelanggan yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika namespace Amazon Redshift Tanpa Server tidak dienkripsi dengan salah satu kunci KMS ini.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

redshift-serverless-publish-logske cloudwatch

Memeriksa apakah Amazon Redshift Server Namespace dikonfigurasi untuk mempublikasikan log berikut ke Amazon Logs. CloudWatch Aturan ini NON_COMPLIANT jika Namespace tidak dikonfigurasi untuk mempublikasikan log berikut ke Amazon Logs. CloudWatch

Pengidentifikasi: REDSHIFT_SERVERLESS_PUBLISH_LOGS_TO_CLOUDWATCH

Jenis Sumber Daya: AWS::RedshiftServerless::Namespace

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (Bahrain), Asia Pasifik (Thailand), Afrika (Cape Town), Asia Pasifik (Hyderabad), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Eropa (Milan), (AS-Timur), AWS GovCloud (AWS GovCloud AS-Barat), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

LogType (Opsional), Jenis: CSV

Daftar tipe log yang dipisahkan koma untuk dipublikasikan ke CloudWatch Log. Nilai yang valid adalah 'connectionlog', 'userlog' Nilai default adalah 'connectionlog', 'userlog'.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

redshift-serverless-workgroup-encrypted-dalam transit

Memeriksa apakah grup kerja AWS Redshift Tanpa Server memiliki parameter konfigurasi require_ssl disetel ke true. Aturannya adalah NON_COMPLIANT jika require_ssl disetel ke false.

Pengidentifikasi: REDSHIFT_SERVERLESS_WORKGROUP_ENCRYPTED_IN_TRANSIT

Jenis Sumber Daya: AWS::RedshiftServerless::Workgroup

Jenis pemicu: Berkala

Wilayah AWS: Hanya tersedia di Eropa (Stockholm), Asia Pasifik (Mumbai), Eropa (Paris), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N), Asia Pasifik (Seoul), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), AS Barat (California N.), Asia Pasifik (Singapura), Asia Pasifik (Sydney)), Kanada (Tengah), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

redshift-serverless-workgroup-no-akses publik

Memeriksa apakah grup kerja Amazon Redshift Tanpa Server tidak mengizinkan akses publik. Aturannya adalah NON_COMPLIANT jika grup kerja mengaktifkan 'Aktifkan Aksesibilitas Publik'.

Pengidentifikasi: REDSHIFT_SERVERLESS_WORKGROUP_NO_PUBLIC_ACCESS

Jenis Sumber Daya: AWS::RedshiftServerless::Workgroup

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (Bahrain), Tiongkok (Beijing), Asia Pasifik (Thailand), Afrika (Cape Town), Asia Pasifik (Hyderabad), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Eropa (Milan), (AS-Timur), (AWS GovCloud AS-Barat), AWS GovCloud Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

redshift-serverless-workgroup-routes-dalam-vpc

Memeriksa apakah grup kerja Amazon Redshift Tanpa Server merutekan lalu lintas jaringan melalui VPC. Aturannya adalah NON_COMPLIANT jika kelompok kerja menonaktifkan 'Aktifkan perutean VPC yang Ditingkatkan'.

Pengidentifikasi: REDSHIFT_SERVERLESS_WORKGROUP_ROUTES_WITHIN_VPC

Jenis Sumber Daya: AWS::RedshiftServerless::Workgroup

Jenis pemicu: Berkala

Wilayah AWS: Hanya tersedia di Eropa (Stockholm), Asia Pasifik (Mumbai), Eropa (Paris), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), AS Timur (Virginia N), Asia Pasifik (Seoul), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), AS Barat (California N.), Asia Pasifik (Singapura), Asia Pasifik (Sydney)), Kanada (Tengah), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

redshift-unrestricted-port-access

Memeriksa apakah grup keamanan yang terkait dengan klaster Amazon Redshift memiliki aturan masuk yang memungkinkan lalu lintas masuk yang tidak dibatasi. Aturannya adalah

NON_COMPLIANT jika ada aturan masuk yang mengizinkan lalu lintas masuk yang tidak dibatasi ke port cluster Redshift.

Pengidentifikasi: REDSHIFT_UNRESTRICTED_PORT_ACCESS

Jenis Sumber Daya: AWS::Redshift::Cluster

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template].

tag yang dibutuhkan

Memeriksa apakah sumber daya Anda memiliki tag yang Anda tentukan. Misalnya, Anda dapat memeriksa apakah EC2 instans Amazon Anda memiliki `CostCenter` tag, sementara juga memeriksa apakah semua instans RDS Anda memiliki satu set tag Keys. Pisahkan beberapa nilai dengan koma. Anda dapat memeriksa hingga 6 tag sekaligus.

Dokumen AWS Systems Manager otomatisasi yang AWS dikelola `AWS-SetRequiredTags` tidak berfungsi sebagai remediasi dengan aturan ini. Anda perlu membuat dokumentasi otomatisasi Systems Manager kustom Anda sendiri untuk remediasi.

Konteks: AWS memungkinkan Anda untuk menetapkan metadata ke AWS sumber daya dalam bentuk tag. Setiap tag adalah label yang terdiri dari kunci dan nilai opsional untuk menyimpan informasi tentang sumber daya atau data yang disimpan pada sumber daya tersebut. Untuk informasi selengkapnya lihat, [Membangun strategi penandaan Anda].

Anda dapat menggunakan aturan ini untuk menemukan sumber daya di akun Anda yang tidak diluncurkan dengan konfigurasi yang Anda inginkan dengan menentukan sumber daya mana yang

harus memiliki tag dan nilai yang diharapkan untuk setiap tag. Anda juga dapat menjalankan tindakan remediasi untuk memperbaiki kesalahan penandaan. Namun, aturan ini tidak mencegah Anda membuat sumber daya dengan tag yang salah.

> **Note**
>
> AWS Config tidak mendukung perekaman tag terkait untuk semua jenis sumber daya. Untuk memverifikasi apakah AWS Config catatan tag dalam item konfigurasi (CI) untuk jenis sumber daya tertentu:
>
> - Periksa apakah AWS Config benar mencatat konfigurasi saat ini untuk sumber daya, tidak termasuk tag.
> - Periksa apakah AWS Config menyegarkan konfigurasi yang direkam saat perubahan dilakukan pada sumber daya.

Pengidentifikasi: REQUIRED_TAGS

Jenis Sumber Daya: AWS::ACM::Certificate AWS::AutoScaling::AutoScalingGroup, AWS::CloudFormation::Stack, AWS::CodeBuild::Project, AWS::DynamoDB::Table, AWS::EC2::CustomerGateway, AWS::EC2::Instance, AWS::EC2::InternetGateway, AWS::EC2::NetworkAcl, AWS::EC2::NetworkInterface, AWS::EC2::RouteTable, AWS::EC2::SecurityGroup AWS::EC2::Subnet, AWS::EC2::Volume, AWS::EC2::VPC, AWS::EC2::VPNConnection, AWS::EC2::VPNGateway, AWS::ElasticLoadBalancing::LoadBalancer, AWS::ElasticLoadBalancingV2::LoadBalancer, AWS::RDS::DBInstance, AWS::RDS::DBSecurityGroup, AWS::RDS::DBSnapshot, AWS::RDS::DBSubnetGroup, AWS::RDS::EventSubscription, AWS::Redshift::Cluster, AWS::Redshift::ClusterParameterGroup, AWS::Redshift::ClusterSecurityGroup, AWS::Redshift::ClusterSnapshot, AWS::Redshift::ClusterSubnetGroup, AWS::S3::Bucket

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

Tag1kunci, Tipe: String, Default: CostCenter

Kunci dari tag yang diperlukan.

Tag1value (Opsional), Jenis: CSV

Nilai opsional dari tag yang diperlukan. Pisahkan beberapa nilai dengan koma.

Tag2key (Opsional), Tipe: String

Kunci dari tag kedua yang diperlukan.

Tag2value (Opsional), Jenis: CSV

Nilai opsional dari tag kedua yang diperlukan. Pisahkan beberapa nilai dengan koma.

Tag3key (Opsional), Tipe: String

Kunci dari tag ketiga yang diperlukan.

Tag3value (Opsional), Jenis: CSV

Nilai opsional dari tag ketiga yang diperlukan. Pisahkan beberapa nilai dengan koma.

Tag4key (Opsional), Tipe: String

Kunci dari tag keempat yang diperlukan.

Tag4value (Opsional), Jenis: CSV

Nilai opsional dari tag keempat yang diperlukan. Pisahkan beberapa nilai dengan koma.

Tag5key (Opsional), Tipe: String

Kunci dari tag kelima yang diperlukan.

Tag5value (Opsional), Jenis: CSV

Nilai opsional dari tag kelima yang diperlukan. Pisahkan beberapa nilai dengan koma.

Tag6key (Opsional), Tipe: String

Kunci dari tag keenam yang diperlukan.

Tag6value (Opsional), Jenis: CSV

Nilai opsional dari tag keenam yang diperlukan. Pisahkan beberapa nilai dengan koma.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

restricted-common-ports

> **Important**
>
> Untuk aturan ini, pengidentifikasi aturan (RESTRICTED_INCOMING_TRAFFIC) dan nama aturan () berbeda. restricted-common-ports

Memeriksa apakah grup keamanan yang digunakan tidak mengizinkan lalu lintas Transmission Control Protocol (TCP) masuk yang tidak dibatasi ke port tertentu. Aturannya adalah COMPLIANT jika:

- Akses port diblokir ke semua lalu lintas TCP.
- Akses port terbuka untuk lalu lintas TCP melalui aturan Inbound, di mana sumbernya adalah satu IPv4 alamat atau rentang alamat dalam notasi CIDR yang tidak mencakup semua IPv4 IPv4 alamat (“0.0.0.0/0").
- Akses port terbuka untuk lalu lintas TCP melalui aturan Inbound, di mana sumbernya adalah satu IPv6 alamat atau rentang IPv6 alamat dalam notasi CIDR yang tidak mencakup semua IPv6 alamat (“:: /0)”).

Aturannya adalah NON_COMPLIANT jika alamat IP untuk koneksi TCP masuk tidak terbatas pada port tertentu.

Pengidentifikasi: RESTRICTED_INCOMING_TRAFFIC

Jenis Sumber Daya: AWS::EC2::SecurityGroup

Jenis pemicu: Perubahan konfigurasi dan Periodik

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

BlockedPort1 (Opsional), Jenis: int, Default: 20

> Nomor port TCP yang diblokir. Default 20 sesuai dengan Transfer Data Transfer Protocol (FTP) Transfer Data Transfer.

BlockedPort2 (Opsional), Jenis: int, Default: 21

Nomor port TCP yang diblokir. Default 21 sesuai dengan Kontrol Perintah File Transfer Protocol (FTP).

BlockedPort3 (Opsional), Jenis: int, Standar: 3389

Nomor port TCP yang diblokir. Default 3389 sesuai dengan Remote Desktop Protocol (RDP).

BlockedPort4 (Opsional), Jenis: int, Standar: 3306

Nomor port TCP yang diblokir. Default 3306 sesuai dengan protokol MySQL.

BlockedPort5 (Opsional), Jenis: int, Standar: 4333

Nomor port TCP yang diblokir. Default 4333 sesuai dengan protokol MySQL.

BlockedPorts (Opsional), Jenis: CSV

Daftar nomor port TCP yang diblokir yang dipisahkan koma. Misalnya, 20, 21, 3306, 3389, dan 4333.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

root-account-hardware-mfa-diaktifkan

Memeriksa apakah AWS akun Anda diaktifkan untuk menggunakan perangkat keras otentikasi multi-faktor (MFA) untuk masuk dengan kredensi root. Aturannya adalah NON_COMPLIANT jika ada perangkat MFA virtual yang diizinkan untuk masuk dengan kredensi root.

> **Note**
>
> Tidak Berlaku untuk Akun Tanpa Kredensi Pengguna Root
> Aturan ini kembali `NOT_APPLICABLE` jika kredensi pengguna root tidak ada.
> Aturan Terkelola dan Jenis Sumber Daya IAM Global
> Jenis sumber daya IAM global yang tersedia sebelum Februari 2022 (`AWS::IAM::Group`,, `AWS::IAM::Policy`AWS::IAM::Role, dan`AWS::IAM::User`) hanya dapat direkam oleh AWS Config di AWS Wilayah yang tersedia sebelum AWS Config Februari 2022. Jenis

sumber daya ini tidak dapat dicatat di Wilayah yang didukung AWS Config setelah Februari 2022. Untuk daftar Wilayah tersebut, lihat Merekam AWS Sumber Daya | Sumber Daya Global.

Jika Anda merekam jenis sumber daya IAM global di setidaknya satu Wilayah, aturan periodik yang melaporkan kepatuhan pada jenis sumber daya IAM global akan menjalankan evaluasi di semua Wilayah di mana aturan periodik ditambahkan, bahkan jika Anda belum mengaktifkan pencatatan jenis sumber daya IAM global di Wilayah tempat aturan periodik ditambahkan.

Untuk menghindari evaluasi yang tidak perlu, Anda hanya harus menerapkan aturan berkala yang melaporkan kepatuhan pada jenis sumber daya IAM global ke salah satu Wilayah yang didukung. Untuk daftar aturan terkelola yang didukung di Wilayah mana, lihat Daftar Aturan AWS Config Terkelola menurut Ketersediaan Wilayah.

Pengidentifikasi: ROOT_ACCOUNT_HARDWARE_MFA_ENABLED

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

root-account-mfa-enabled

Memeriksa apakah pengguna root AWS akun Anda memerlukan otentikasi multi-faktor untuk login konsol. Aturannya adalah NON_COMPLIANT jika pengguna akun root AWS Identity and Access Management (IAM) and Access Management (IAM) tidak mengaktifkan multi-factor authentication (MFA).

> **Note**
>
> Tidak Berlaku untuk Akun Tanpa Kredensi Pengguna Root
>
> Aturan ini kembali `NOT_APPLICABLE` jika kredensi pengguna root tidak ada.
>
> Aturan Terkelola dan Jenis Sumber Daya IAM Global
>
> Jenis sumber daya IAM global yang tersedia sebelum Februari 2022 (`AWS::IAM::Group`,, `AWS::IAM::PolicyAWS::IAM::Role`, dan`AWS::IAM::User`) hanya dapat direkam oleh AWS Config di AWS Wilayah yang tersedia sebelum AWS Config Februari 2022. Jenis sumber daya ini tidak dapat dicatat di Wilayah yang didukung AWS Config setelah Februari 2022. Untuk daftar Wilayah tersebut, lihat Merekam AWS Sumber Daya | Sumber Daya Global.
>
> Jika Anda merekam jenis sumber daya IAM global di setidaknya satu Wilayah, aturan periodik yang melaporkan kepatuhan pada jenis sumber daya IAM global akan menjalankan evaluasi di semua Wilayah di mana aturan periodik ditambahkan, bahkan jika Anda belum mengaktifkan pencatatan jenis sumber daya IAM global di Wilayah tempat aturan periodik ditambahkan.
>
> Untuk menghindari evaluasi yang tidak perlu, Anda hanya harus menerapkan aturan berkala yang melaporkan kepatuhan pada jenis sumber daya IAM global ke salah satu Wilayah yang didukung. Untuk daftar aturan terkelola yang didukung di Wilayah mana, lihat Daftar Aturan AWS Config Terkelola menurut Ketersediaan Wilayah.

Pengidentifikasi: ROOT_ACCOUNT_MFA_ENABLED

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

rute53- query-logging-enabled

Memeriksa apakah pencatatan kueri DNS diaktifkan untuk zona host publik Amazon Route 53 Anda. Aturannya adalah NON_COMPLIANT jika pencatatan kueri DNS tidak diaktifkan untuk zona host publik Amazon Route 53 Anda.

Pengidentifikasi: _QUERY_LOGGING_ENABLED ROUTE53

Jenis Sumber Daya: AWS::Route53::HostedZone

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Wilayah AS Timur (Virginia Utara)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

s3 -aturan-periksa express-dir-bucket-lifecycle

Memeriksa apakah aturan siklus hidup dikonfigurasi untuk bucket direktori Amazon S3 Express. Aturannya adalah NON_COMPLIANT jika tidak ada aturan konfigurasi siklus hidup aktif atau konfigurasi tidak cocok dengan nilai parameter.

Pengidentifikasi: S3EXPRESS_DIR_BUCKET_LIFECYCLE_RULES_CHECK

Jenis Sumber Daya: AWS::S3Express::DirectoryBucket

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Eropa (Stockholm), Asia Pasifik (Mumbai), AS Timur (Ohio), Eropa (Irlandia), AS Timur (Virginia N.), Asia Pasifik (Tokyo), Wilayah AS Barat (Oregon)

Parameter:

targetExpirationDays (Opsional), Jenis: int

Jumlah hari setelah pembuatan ketika objek dihapus dari ember direktori Amazon S3 Express.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

s3- -hanya access-point-in-vpc

Memeriksa apakah jalur akses Amazon S3 tidak mengizinkan akses dari internet (adalah NetworkOrigin VPC). Aturannya adalah NON_COMPLIANT jika NetworkOrigin Internet.

Pengidentifikasi: S3_ACCESS_POINT_IN_VPC_ONLY

Jenis Sumber Daya: AWS::S3::AccessPoint

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

s3- -blok access-point-public-access

Memeriksa apakah titik akses Amazon S3 telah mengaktifkan pengaturan akses publik blok. Aturannya adalah NON_COMPLIANT jika pengaturan akses publik blok tidak diaktifkan untuk titik akses S3.

Pengidentifikasi: S3_ACCESS_POINT_PUBLIC_ACCESS_BLOCKS

Jenis Sumber Daya: AWS::S3::AccessPoint

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

excludedAccessPoints (Opsional), Jenis: CSV

Daftar nama yang dipisahkan koma untuk jalur akses Amazon S3 publik yang diizinkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

s3- -blok account-level-public-access

Memeriksa apakah pengaturan blok akses publik yang diperlukan dikonfigurasi dari tingkat akun. Aturannya hanya NON_COMPLIANT jika bidang yang ditetapkan di bawah ini tidak cocok dengan bidang yang sesuai di item konfigurasi.

> **Note**
>
> Jika Anda menggunakan aturan ini, pastikan bahwa S3 Block Public Access diaktifkan. Aturan ini dipicu oleh perubahan, sehingga tidak akan dipanggil kecuali S3 Block Public Access diaktifkan. Jika S3 Block Public Access tidak diaktifkan aturan mengembalikan INSUFFICIENT_DATA. Ini berarti bahwa Anda mungkin masih memiliki beberapa ember publik. Untuk informasi selengkapnya tentang mengatur Akses Publik Blok S3, lihat [Memblokir akses publik ke penyimpanan Amazon S3 Anda](#).

Pengidentifikasi: S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS

Jenis Sumber Daya: AWS::S3::AccountPublicAccessBlock

Jenis pemicu: Perubahan konfigurasi (status saat ini tidak dicentang, hanya dievaluasi saat perubahan menghasilkan peristiwa baru)

> **Note**
>
> Aturan ini hanya dipicu oleh perubahan konfigurasi untuk wilayah tertentu tempat titik akhir S3 berada. Di semua wilayah lain, aturan diperiksa secara berkala. Jika perubahan dibuat di wilayah lain, mungkin ada penundaan sebelum aturan mengembalikan NON_COMPLIANT.

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

IgnorePublicAcls (Opsional), Tipe: String, Bawaan: BETUL

IgnorePublicAcls diberlakukan atau tidak, default Benar

BlockPublicPolicy (Opsional), Tipe: String, Bawaan: BETUL

BlockPublicPolicy diberlakukan atau tidak, default Benar

BlockPublicAcls (Opsional), Tipe: String, Bawaan: BETUL

BlockPublicAcls diberlakukan atau tidak, default Benar

RestrictPublicBuckets (Opsional), Tipe: String, Bawaan: BETUL

RestrictPublicBuckets diberlakukan atau tidak, default Benar

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

s3- account-level-public-access -blok-periodik

Memeriksa apakah pengaturan blok akses publik yang diperlukan dikonfigurasi di tingkat akun. Aturannya adalah NON_COMPLIANT jika item konfigurasi tidak cocok dengan satu atau beberapa pengaturan dari parameter (atau default).

Pengidentifikasi: S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC

Jenis Sumber Daya: AWS: :::Akun

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

IgnorePublicAcls (Opsional), Tipe: String

IgnorePublicAcls diberlakukan atau tidak, default Benar

BlockPublicPolicy (Opsional), Tipe: String

BlockPublicPolicy diberlakukan atau tidak, default Benar

BlockPublicAcls (Opsional), Tipe: String

BlockPublicAcls diberlakukan atau tidak, default Benar

RestrictPublicBuckets (Opsional), Tipe: String

RestrictPublicBuckets diberlakukan atau tidak, default Benar

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

s3- bucket-acl-prohibited

Memeriksa apakah Amazon Simple Storage Service (Amazon S3) Bucket mengizinkan izin pengguna melalui daftar kontrol akses (). ACLs Aturannya adalah NON_COMPLIANT jika ACLs dikonfigurasi untuk akses pengguna di Amazon S3 Bucket.

Pengidentifikasi: S3_BUCKET_ACL_FORBIDNED

Jenis Sumber Daya: AWS::S3::Bucket

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

s3- bucket-blacklisted-actions-prohibited

Memeriksa apakah kebijakan bucket Amazon Simple Storage Service (Amazon S3) tidak mengizinkan tindakan tingkat ember dan tingkat objek yang diblokir pada sumber daya dalam bucket untuk prinsipal dari akun lain. AWS Misalnya, aturan memeriksa bahwa kebijakan bucket Amazon S3 tidak mengizinkan AWS akun lain untuk melakukan `s3:GetBucket*` tindakan apa pun dan `s3:DeleteObject` pada objek apa pun di bucket. Aturannya adalah NON_COMPLIANT jika ada tindakan yang diblokir yang diizinkan oleh kebijakan bucket Amazon S3.

> **Note**
>
> Aturan hanya akan memeriksa entitas di properti Principal dan tidak memperhitungkan persyaratan apa pun di bawah properti Condition dalam kebijakan

Pengidentifikasi: S3_BUCKET_BLACKLISTED_ACTIONS_FORBIDNED

Jenis Sumber Daya: AWS::S3::Bucket

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Hyderabad), Eropa (Spanyol)

Parameter:

blacklistedActionPattern, Jenis: CSV

Daftar pola tindakan daftar hitam yang dipisahkan koma, misalnya, s3: GetBucket * dan s3:. DeleteObject

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

s3- -diaktifkan bucket-cross-region-replication

Memeriksa apakah Anda telah mengaktifkan Replikasi Lintas Wilayah S3 untuk bucket Amazon S3 Anda. Aturannya adalah NON_COMPLIANT jika tidak ada aturan replikasi yang diaktifkan untuk Replikasi Lintas Wilayah.

Pengidentifikasi: S3_BUCKET_CROSS_REGION_REPLICATION_ENABLED

Jenis Sumber Daya: AWS::S3::Bucket

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

s3- bucket-default-lock-enabled

Memeriksa apakah bucket S3 telah mengaktifkan kunci, secara default. Aturannya adalah NON_COMPLIANT jika kunci tidak diaktifkan.

Pengidentifikasi: S3_BUCKET_DEFAULT_LOCK_ENABLED

Jenis Sumber Daya: AWS::S3::Bucket

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

mode (Opsional), Tipe: String

mode: (opsional): Parameter mode dengan nilai tata kelola atau KEPATUHAN yang valid.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

s3- -dilarang bucket-level-public-access

Memeriksa apakah bucket S3 dapat diakses publik. Aturannya adalah NON_COMPLIANT jika bucket S3 tidak tercantum dalam `excludedPublicBuckets` parameter dan pengaturan tingkat bucket bersifat publik.

Pengidentifikasi: S3_BUCKET_LEVEL_PUBLIC_ACCESS_FORBEDDED

Jenis Sumber Daya: AWS::S3::Bucket

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

excludedPublicBuckets (Opsional), Jenis: CSV

Daftar terpisah koma dari nama bucket Amazon S3 publik yang diizinkan yang diketahui.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

s3- bucket-logging-enabled

Memeriksa apakah logging diaktifkan untuk bucket S3 Anda. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan.

Pengidentifikasi: S3_BUCKET_LOGGING_ENABLED

Jenis Sumber Daya: AWS::S3::Bucket

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

TargetBucket (Opsional), Tipe: String

Targetkan bucket S3 untuk menyimpan log akses server.

TargetPrefix (Opsional), Tipe: String

Awalan bucket S3 untuk menyimpan log akses server.

Evaluasi Proaktif

Untuk langkah-langkah tentang cara menjalankan aturan ini dalam mode proaktif, lihat Mengevaluasi Sumber Daya Anda dengan AWS Config Aturan. Agar aturan ini mengembalikan COMPLIANT dalam mode proaktif, skema konfigurasi sumber daya untuk StartResourceEvaluationAPI harus menyertakan input berikut, yang dikodekan sebagai string:

```
"ResourceConfiguration":
...
{
   "BucketName": "amzn-s3-demo-bucket",
   "LoggingConfiguration": {
         "DestinationBucketName": "amzn-s3-demo-destination-bucket",
         "LogFilePrefix":"my-log"
   }
}
...
```

Untuk informasi lebih lanjut tentang evaluasi proaktif, lihat Mode Evaluasi.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

s3- bucket-mfa-delete-enabled

Memeriksa apakah MFA Delete diaktifkan di konfigurasi pembuatan versi bucket Amazon Simple Storage Service (Amazon S3). Aturannya adalah NON_COMPLIANT jika MFA Delete tidak diaktifkan.

Pengidentifikasi: S3_BUCKET_MFA_DELETE_ENABLED

Jenis Sumber Daya: AWS::S3::Bucket

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

s3- bucket-policy-grantee-check

Memeriksa bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh salah satu AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau yang Anda berikan. VPCs Aturannya SESUAI jika kebijakan bucket tidak ada.

Misalnya, jika parameter input ke aturan adalah daftar dua prinsip: `111122223333` `444455556666` dan kebijakan bucket menetapkan bahwa hanya `111122223333` dapat mengakses bucket, maka aturannya adalah COMPLIANT. Dengan parameter input yang sama: Jika kebijakan bucket menentukan itu `111122223333` dan `444455556666` dapat mengakses bucket, itu juga COMPLIANT.

Namun, jika kebijakan bucket menentukan yang `999900009999` dapat mengakses bucket, aturannya adalah NON_COMPLIANT.

> **Note**
>
> Jika kebijakan bucket berisi lebih dari satu pernyataan, setiap pernyataan dalam kebijakan bucket dievaluasi berdasarkan aturan ini.

Pengidentifikasi: S3_BUCKET_POLICY_GRANTEE_CHECK

Jenis Sumber Daya: AWS::S3::Bucket

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei)

Parameter:

AWSprincipals (Opsional), Jenis: CSV

Daftar prinsipal yang dipisahkan koma seperti Pengguna IAM, Peran IAM ARNs, dan akun. ARNs AWS Anda harus memberikan ARN penuh atau menggunakan pencocokan sebagian. Misalnya, “arn:aws:iam: ::role/" atau “arn:aws:iam: ::role/*`AccountID`”. `role_name` `AccountID` Jika nilai yang diberikan tidak sama persis dengan ARN utama yang ditentukan dalam kebijakan bucket, aturannya adalah NON_COMPLIANT.

ServicePrincipals (Opsional), Jenis: CSV

Daftar prinsip layanan yang dipisahkan koma, misalnya 'cloudtrail.amazonaws.com, lambda.amazonaws.com'.

FederatedUsers (Opsional), Jenis: CSV

Daftar penyedia identitas yang dipisahkan koma untuk federasi identitas web seperti Amazon Cognito dan penyedia identitas SAM. Misalnya 'cognito-identity.amazonaws.com, arn:aws:iam: :111122223333:saml-provider/my-provider'.

IPAdDdresses (Opsional), Jenis: CSV

Daftar alamat IP berformat CIDR yang dipisahkan koma, misalnya '10.0.0.1, 192.168.1.0/24, 2001:db8: :/32'.

VPCIDS (Opsional), Jenis: CSV

Daftar Amazon Virtual Private Clouds (Amazon VPC) yang dipisahkan koma, misalnya 'vpc-1234abc0 IDs, vpc-ab1234c0'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

s3- bucket-policy-not-more -permisif

Memeriksa apakah kebijakan bucket Amazon Simple Storage Service tidak mengizinkan izin antar akun selain kebijakan bucket Amazon S3 kontrol yang Anda berikan.

> **Note**
>
> Jika Anda memberikan nilai parameter yang tidak valid, Anda akan melihat kesalahan berikut: Nilai untuk parameter ControlPolicy harus berupa kebijakan bucket Amazon S3.

Pengidentifikasi: S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE

Jenis Sumber Daya: AWS::S3::Bucket

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei)

Parameter:

controlPolicy, Tipe: String

Kebijakan bucket Amazon S3 yang menentukan batas atas izin bucket S3 Anda. Panjangnya bisa maksimal 1024 karakter.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

s3- bucket-public-read-prohibited

Memeriksa apakah bucket Amazon S3 Anda tidak mengizinkan akses baca publik. Aturan memeriksa pengaturan Blokir Akses Publik, kebijakan bucket, dan daftar kontrol akses bucket (ACL).

Aturan ini sesuai jika kedua hal berikut ini benar:

- Pengaturan Blokir Akses Publik membatasi kebijakan publik atau kebijakan bucket tidak mengizinkan akses baca publik.
- Pengaturan Blokir Akses Publik membatasi publik ACLs atau bucket ACL tidak mengizinkan akses baca publik.

Aturannya tidak patuh ketika:

- Jika setelan Blokir Akses Publik tidak membatasi kebijakan publik, AWS Config evaluasi apakah kebijakan tersebut mengizinkan akses baca publik. Jika kebijakan mengizinkan akses baca publik, aturannya tidak sesuai.
- Jika setelan Blokir Akses Publik tidak membatasi bucket publik ACLs, AWS Config evaluasi apakah bucket ACL mengizinkan akses baca publik. Jika bucket ACL mengizinkan akses baca publik, aturannya tidak sesuai.

> **Note**
>
> Agar dianggap non-publik, kebijakan bucket S3 harus memberikan akses hanya ke nilai tetap. Ini berarti nilai yang tidak mengandung wildcard atau elemen kebijakan IAM berikut: Variabel.

Pengidentifikasi: S3_BUCKET_PUBLIC_READ_FORBIDNED

Jenis Sumber Daya: AWS::S3::Bucket

Jenis pemicu: Perubahan konfigurasi dan Periodik

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

s3- bucket-public-write-prohibited

Memeriksa apakah bucket Amazon S3 Anda tidak mengizinkan akses tulis publik. Aturan memeriksa pengaturan Blokir Akses Publik, kebijakan bucket, dan daftar kontrol akses bucket (ACL).

Aturan ini sesuai jika kedua hal berikut ini benar:

- Pengaturan Blokir Akses Publik membatasi kebijakan publik atau kebijakan bucket tidak mengizinkan akses tulis publik.

- Pengaturan Blokir Akses Publik membatasi publik ACLs atau bucket ACL tidak mengizinkan akses tulis publik.

Aturannya tidak patuh ketika:

- Jika setelan Blokir Akses Publik tidak membatasi kebijakan publik, AWS Config evaluasi apakah kebijakan tersebut mengizinkan akses tulis publik. Jika kebijakan mengizinkan akses tulis publik, aturannya tidak sesuai.
- Jika setelan Blokir Akses Publik tidak membatasi bucket publik ACLs, AWS Config evaluasi apakah bucket ACL mengizinkan akses tulis publik. Jika bucket ACL mengizinkan akses tulis publik, aturannya tidak sesuai.

> **Note**
>
> Aturan ini tidak mengevaluasi perubahan pada akses blok publik tingkat akun. Untuk memeriksa apakah pengaturan blok akses publik yang diperlukan dikonfigurasi dari tingkat akun, lihat s3- account-level-public-access -blocks dan s3 - -blocks-periodik. account-level-public-access

> **Note**
>
> Agar dianggap non-publik, kebijakan bucket S3 harus memberikan akses hanya ke nilai tetap. Ini berarti nilai yang tidak mengandung wildcard atau elemen kebijakan IAM berikut: Variabel.

Pengidentifikasi: S3_BUCKET_PUBLIC_WRITE_FORBIDNED

Jenis Sumber Daya: AWS::S3::Bucket

Jenis pemicu: Perubahan konfigurasi dan Periodik

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

s3- bucket-replication-enabled

Memeriksa apakah bucket S3 mengaktifkan aturan replikasi. Aturannya adalah NON_COMPLIANT jika bucket S3 tidak memiliki aturan replikasi atau memiliki aturan replikasi yang tidak diaktifkan.

Pengidentifikasi: S3_BUCKET_REPLICATION_ENABLED

Jenis Sumber Daya: AWS::S3::Bucket

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

ReplicationType (Opsional), Tipe: String

> Nilai yang diterima: 'CROSS-REGION' dan 'SAME-REGION'. Masukkan 'CROSS-REGION' untuk aturan untuk memeriksa bahwa semua bucket hanya mengaktifkan Replikasi Lintas Wilayah. Masukkan 'SAME-REGION' untuk aturan untuk memeriksa bahwa semua bucket hanya mengaktifkan Replikasi Wilayah yang Sama.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

s3- -diaktifkan bucket-server-side-encryption

Memeriksa apakah bucket Amazon S3 Anda mengaktifkan enkripsi default Amazon S3 atau kebijakan bucket Amazon S3 secara eksplisit `put-object` menolak permintaan tanpa enkripsi sisi server yang menggunakan AES-256 atau. AWS Key Management Service Aturannya adalah NON_COMPLIANT jika bucket Amazon S3 Anda tidak dienkripsi secara default.

Pengidentifikasi: S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED

Jenis Sumber Daya: AWS::S3::Bucket

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Eropa (Spanyol)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

s3- bucket-ssl-requests-only

Memeriksa apakah bucket S3 memiliki kebijakan yang mengharuskan permintaan untuk menggunakan SSL/TLS. Aturannya adalah NON_COMPLIANT jika ada bucket S3 yang memiliki kebijakan yang mengizinkan permintaan HTTP.

Pengidentifikasi: S3_BUCKET_SSL_REQUESTS_ONLY

Jenis Sumber Daya: AWS::S3::Bucket

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

s3-ember dengan tag

Memeriksa apakah bucket Amazon S3 memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: S3_BUCKET_TAGGED

Jenis Sumber Daya: AWS::S3::Bucket

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

s3- bucket-versioning-enabled

Memeriksa apakah pembuatan versi diaktifkan untuk bucket S3 Anda. Secara opsional, aturan memeriksa apakah penghapusan MFA diaktifkan untuk bucket S3 Anda.

Pengidentifikasi: S3_BUCKET_VERSIONING_ENABLED

Jenis Sumber Daya: AWS::S3::Bucket

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

isMfaDeleteDiaktifkan (Opsional), Tipe: String

> Penghapusan MFA diaktifkan untuk bucket S3 Anda.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

s3- default-encryption-kms

Memeriksa apakah bucket S3 dienkripsi dengan AWS Key Management Service (KMS).AWS Aturannya adalah NON_COMPLIANT jika bucket S3 tidak dienkripsi dengan kunci KMS. AWS

Pengidentifikasi: S3_DEFAULT_ENCRYPTION_KMS

Jenis Sumber Daya: AWS::S3::Bucket, AWS::KMS::Key

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei)

Parameter:

kmsKeyArns (Opsional), Jenis: CSV

> Daftar kunci AWS KMS yang dipisahkan koma ARNs diizinkan untuk mengenkripsi Bucket Amazon S3.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

s3- event-notifications-enabled

Memeriksa apakah Pemberitahuan Acara Amazon S3 diaktifkan pada bucket S3. Aturannya adalah NON_COMPLIANT jika Pemberitahuan Acara S3 tidak disetel pada bucket, atau jika jenis acara atau tujuan tidak cocok dengan parameter dan destinationARN. `eventTypes`

Pengidentifikasi: S3_EVENT_NOTIFICATIONS_ENABLED

Jenis Sumber Daya: AWS::S3::Bucket

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

DestinationARN (Opsional), Tipe: String

Nama Sumber Daya Amazon (ARN) tujuan pemberitahuan acara (topik Amazon SNS, AWS Lambda, Antrian Amazon SQS).

EventTypes (Opsional), Jenis: CSV

Daftar terpisah koma dari jenis acara Amazon S3 pilihan

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

s3- -dibuat last-backup-recovery-point

Memeriksa apakah titik pemulihan dibuat untuk Amazon Simple Storage Service (Amazon S3) Simple Storage S3). Aturannya adalah NON_COMPLIANT jika bucket Amazon S3 tidak memiliki titik pemulihan terkait yang dibuat dalam periode waktu yang ditentukan.

Pengidentifikasi: S3_LAST_BACKUP_RECOVERY_POINT_CREATED

Jenis Sumber Daya: AWS::S3::Bucket

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

ResourceTags (Opsional), Tipe: String

Tag bucket Amazon S3 untuk aturan yang akan diperiksa, dalam format JSON. `{"tagkey" : "tagValue"}`

ResourceID (Opsional), Tipe: String

Nama bucket Amazon S3 untuk diperiksa aturan.

recoveryPointAgeNilai (Opsional), Jenis: int, Default: 1

Nilai numerik untuk usia maksimum yang diizinkan. Tidak lebih dari 744 jam, 31 untuk hari.

recoveryPointAgeUnit (Opsional), Tipe: String, Default: hari

Satuan waktu untuk usia maksimum yang diizinkan. Nilai yang diterima: 'jam', 'hari'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

s3- lifecycle-policy-check

Memeriksa apakah aturan siklus hidup dikonfigurasi untuk bucket Amazon Simple Storage Service (Amazon S3). Aturannya adalah NON_COMPLIANT jika tidak ada aturan konfigurasi siklus hidup aktif atau konfigurasi tidak cocok dengan nilai parameter.

Pengidentifikasi: S3_LIFECYCLE_POLICY_CHECK

Jenis Sumber Daya: AWS::S3::Bucket

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

targetTransitionDays (Opsional), Jenis: int

Jumlah hari setelah pembuatan objek ketika objek dialihkan ke kelas penyimpanan tertentu (misalnya, 30 hari).

targetExpirationDays (Opsional), Jenis: int

Jumlah hari setelah pembuatan objek ketika objek dihapus (misalnya, 395 hari).

targetTransitionStorageKelas (Opsional), Tipe: String

Jenis kelas penyimpanan tujuan. Misalnya, Akses Jarang Standar Amazon S3 (IA Standar S3). Untuk informasi selengkapnya, lihat Memahami dan mengelola kelas penyimpanan Amazon S3.

TargetPrefix (Opsional), Tipe: String

Awalan Objek Amazon S3 untuk mengidentifikasi satu atau beberapa objek.

BucketNames (Opsional), Jenis: CSV

Daftar nama bucket Amazon S3 yang dipisahkan koma yang mengaktifkan kebijakan siklus hidup.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

s3- meets-restore-time-target

Memeriksa apakah waktu pemulihan bucket Amazon Simple Storage Service (Amazon S3) memenuhi durasi yang ditentukan. Aturannya adalah NON_COMPLIANT jika bucket Amazon S3 lebih besar LatestRestoreExecutionTimeMinutes dari menit. maxRestoreTime

Pengidentifikasi: S3_MEETS_RESTORE_TIME_TARGET

Jenis Sumber Daya: AWS::S3::Bucket

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

maxRestoreTime, Jenis: int

Nilai numerik untuk runtime pemulihan maksimum yang diizinkan.

ResourceTags (Opsional), Tipe: String

Tag bucket Amazon S3 untuk aturan yang akan diperiksa, dalam format JSON.

ResourceID (Opsional), Tipe: String

Nama bucket Amazon S3 untuk diperiksa aturan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

s3- resources-in-logically-air -gapped-lemari besi

Memeriksa apakah bucket Amazon Simple Storage Service (Amazon S3) berada dalam brankas yang memiliki lubang udara secara logis. Aturannya adalah NON_COMPLIANT jika bucket Amazon S3 tidak berada dalam brankas yang memiliki lubang udara secara logis dalam periode waktu yang ditentukan.

Pengidentifikasi: S3_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

Jenis Sumber Daya: AWS::S3::Bucket

Jenis pemicu: Berkala

Wilayah AWS: Hanya tersedia di Eropa (Stockholm), Timur Tengah (Bahrain), Asia Pasifik (Mumbai), Eropa (Paris), AS Timur (Ohio), Eropa (Irlandia), Eropa (Frankfurt), Amerika Selatan (Sao Paulo), AS Timur (Virginia N.), Asia Pasifik (Seoul), Asia Pasifik (Osaka), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), AS Barat (California N.), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Wilayah Kanada (Tengah)

Parameter:

ResourceTags (Opsional), Tipe: String

Tag bucket Amazon S3 untuk aturan yang akan diperiksa, dalam format JSON.

ResourceID (Opsional), Tipe: String

Nama bucket Amazon S3 untuk diperiksa aturan.

recoveryPointAgeNilai (Opsional), Jenis: int, Default: 1

Nilai numerik untuk usia maksimum yang diizinkan. Tidak lebih dari 2184 jam, 91 untuk hari.

recoveryPointAgeUnit (Opsional), Tipe: String, Default: hari

Satuan waktu untuk usia maksimum yang diizinkan. Nilai yang diterima: 'jam', 'hari'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

s3- -rencana resources-protected-by-backup

Memeriksa apakah bucket Amazon Simple Storage Service (Amazon S3) dilindungi oleh paket cadangan. Aturannya adalah NON_COMPLIANT jika bucket Amazon S3 tidak tercakup oleh paket cadangan.

Pengidentifikasi: S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Jenis Sumber Daya: AWS::S3::Bucket

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

ResourceTags (Opsional), Tipe: String

Tag untuk bucket Amazon S3 untuk aturan yang akan diperiksa, dalam format JSON. `{"tagkey" : "tagValue"}`

ResourceID (Opsional), Tipe: String

Nama bucket Amazon S3 untuk diperiksa aturan.

crossRegionList (Opsional), Tipe: String

Daftar wilayah tujuan yang dipisahkan koma untuk salinan cadangan lintas wilayah yang akan disimpan

crossAccountList (Opsional), Tipe: String

Daftar akun tujuan yang dipisahkan koma untuk salinan cadangan lintas akun yang akan disimpan

maxRetentionDays (Opsional), Jenis: int

Periode retensi maksimum dalam beberapa hari untuk Backup Vault Lock

minRetentionDays (Opsional), Jenis: int

Periode retensi minimum dalam beberapa hari untuk Backup Vault Lock

backupVaultLockPeriksa (Opsional), Tipe: String

Nilai yang diterima: 'Benar' atau 'False'. Masukkan 'Benar' untuk aturan untuk memeriksa apakah sumber daya dicadangkan di brankas yang terkunci

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

s3- version-lifecycle-policy-check

Memeriksa apakah bucket yang diaktifkan versi Amazon Simple Storage Service (Amazon S3) memiliki kebijakan siklus hidup yang dikonfigurasi. Aturannya adalah NON_COMPLIANT jika kebijakan siklus hidup Amazon S3 tidak diaktifkan.

Pengidentifikasi: S3_VERSION_LIFECYCLE_POLICY_CHECK

Jenis Sumber Daya: AWS::S3::Bucket

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

BucketNames (Opsional), Jenis: CSV

Daftar nama bucket Amazon S3 yang dipisahkan koma yang mengaktifkan kebijakan siklus hidup.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

sagemaker-app-image-config-ditandai

Memeriksa apakah konfigurasi gambar SageMaker aplikasi Amazon memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: SAGEMAKER_APP_IMAGE_CONFIG_TAGGED

Jenis Sumber Daya: AWS::SageMaker::AppImageConfig

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

sagemaker-domain-in-vpc

Memeriksa apakah SageMaker domain Amazon menggunakan Amazon Virtual Private Cloud (VPC) milik pelanggan untuk lalu lintas non-EFS. Aturannya adalah NON_COMPLIANT jika konfigurasi. AppNetworkAccessType tidak diatur ke VpcOnly.

Pengidentifikasi: SAGEMAKER_DOMAIN_IN_VPC

Jenis Sumber Daya: AWS::SageMaker::Domain

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

sagemaker-domain-tagged

Memeriksa apakah SageMaker domain Amazon memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: SAGEMAKER_DOMAIN_TAGGED

Jenis Sumber Daya: AWS::SageMaker::Domain

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi

Memeriksa apakah AWS kunci Key Management Service (AWS KMS) dikonfigurasi untuk konfigurasi SageMaker endpoint Amazon. Aturannya adalah NON_COMPLIANT jika 'KmsKeyId' tidak ditentukan untuk konfigurasi titik akhir Amazon SageMaker .

Pengidentifikasi: SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURATED

Jenis Sumber Daya: AWS::SageMaker::EndpointConfig

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Wilayah Asia Pasifik (Taipei)

Parameter:

kmsKeyArns (Opsional), Tipe: String

> Daftar kunci AWS KMS tertentu yang dipisahkan koma ARNs diizinkan untuk konfigurasi titik akhir Amazon SageMaker .

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

sagemaker-endpoint-config-prod-hitungan contoh

Memeriksa apakah konfigurasi SageMaker endpoint Amazon memiliki varian produksi `InitialInstanceCount` disetel ke nilai yang lebih besar dari 1. Aturannya adalah NON_COMPLIANT jika varian produksi `InitialInstanceCount` sama dengan 1.

Pengidentifikasi: SAGEMAKER_ENDPOINT_CONFIG_PROD_INSTANCE_COUNT

Jenis Sumber Daya: AWS::SageMaker::EndpointConfig

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

sagemaker-feature-group-tagged

Memeriksa apakah grup SageMaker fitur Amazon memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: SAGEMAKER_FEATURE_GROUP_TAGGED

Jenis Sumber Daya: AWS::SageMaker::FeatureGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Tiongkok (Ningxia), Eropa (Zurich) Wilayah

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

sagemaker-image-description

Memeriksa apakah SageMaker gambar Amazon memiliki deskripsi. Aturannya adalah NON_COMPLIANT jika konfigurasi. ImageDescription tidak ada.

Pengidentifikasi: SAGEMAKER_IMAGE_DESCRIPTION

Jenis Sumber Daya: AWS::SageMaker::Image

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

sagemaker-image-tagged

Memeriksa apakah SageMaker gambar Amazon memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: SAGEMAKER_IMAGE_TAGGED

Jenis Sumber Daya: AWS::SageMaker::Image

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

sagemaker-model-in-vpc

Memeriksa apakah SageMaker model Amazon menggunakan Amazon Virtual Private Cloud (Amazon VPC) untuk lalu lintas kontainer. Aturannya adalah NON_COMPLIANT jika konfigurasi. VpcConfig tidak ada.

Pengidentifikasi: SAGEMAKER_MODEL_IN_VPC

Jenis Sumber Daya: AWS::SageMaker::Model

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

sagemaker-model-isolation-enabled

Memeriksa apakah SageMaker model Amazon mengaktifkan isolasi jaringan. Aturannya adalah NON_COMPLIANT jika konfigurasi. EnableNetworkIsolation adalah palsu.

Pengidentifikasi: SAGEMAKER_MODEL_ISOLATION_ENABLED

Jenis Sumber Daya: AWS::SageMaker::Model

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Tiongkok (Beijing), Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

sagemaker-notebook-instance-inside-vpc

Memeriksa apakah instans SageMaker notebook Amazon diluncurkan dalam VPC atau dalam daftar subnet yang disetujui. Aturannya adalah NON_COMPLIANT jika instance notebook tidak diluncurkan dalam VPC atau jika ID subnetnya tidak disertakan dalam daftar parameter.

Pengidentifikasi: SAGEMAKER_NOTEBOOK_INSTANCE_INSIDE_VPC

Jenis Sumber Daya: AWS::SageMaker::NotebookInstance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur), AWS GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Eropa (Zurich) Wilayah

Parameter:

SubnetIds (Opsional), Jenis: CSV

Daftar subnet IDs yang dipisahkan koma tempat instance notebook dapat diluncurkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

sagemaker-notebook-instance-kms-kunci-dikonfigurasi

Memeriksa apakah AWS kunci Key Management Service (AWS KMS) dikonfigurasi untuk instance SageMaker notebook Amazon. Aturannya adalah NON_COMPLIANT jika 'KmsKeyId' tidak ditentukan untuk instance notebook. SageMaker

Pengidentifikasi: SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURATED

Jenis Sumber Daya: AWS::SageMaker::NotebookInstance

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Wilayah Asia Pasifik (Taipei)

Parameter:

kmsKeyArns (Opsional), Tipe: String

Daftar kunci AWS KMS yang dipisahkan koma ARNs diizinkan untuk instance notebook Amazon SageMaker .

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

sagemaker-notebook-instance-platform-versi

Memeriksa apakah Instance Notebook Sagemaker dikonfigurasi untuk menggunakan versi pengenal platform yang didukung. Aturannya adalah NON_COMPLIANT jika Instance Notebook tidak menggunakan versi pengenal platform yang didukung yang ditentukan seperti yang ditentukan dalam parameter.

Pengidentifikasi: SAGEMAKER_NOTEBOOK_INSTANCE_PLATFORM_VERSION

Jenis Sumber Daya: AWS::SageMaker::NotebookInstance

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (Bahrain), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

supportedPlatformIdentifierVersi, Jenis: CSV

Daftar dipisahkan koma dari versi pengenal platform yang didukung untuk diperiksa aturan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

sagemaker-notebook-instance-root-akses-cek

Memeriksa apakah SageMaker RootAccess setelan Amazon diaktifkan untuk instans SageMaker notebook Amazon. Aturannya adalah NON_COMPLIANT jika RootAccess setelan disetel ke 'Diaktifkan' untuk instance notebook Amazon SageMaker .

Pengidentifikasi: SAGEMAKER_NOTEBOOK_INSTANCE_ROOT_ACCESS_CHECK

Jenis Sumber Daya: AWS::SageMaker::NotebookInstance

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur), AWS

GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Eropa (Zurich) Wilayah

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

sagemaker-notebook-no-direct-akses internet

Memeriksa apakah akses internet langsung dinonaktifkan untuk instance SageMaker notebook Amazon. Aturannya adalah NON_COMPLIANT jika instance SageMaker notebook diaktifkan internet.

Pengidentifikasi: SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS

Jenis Sumber Daya: AWS::SageMaker::NotebookInstance

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Wilayah Asia Pasifik (Taipei)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

secretsmanager-rotation-enabled-check

Memeriksa apakah AWS rahasia Secrets Manager telah mengaktifkan rotasi. Aturan ini juga memeriksa `maximumAllowedRotationFrequency` parameter opsional. Jika parameter ditentukan, frekuensi rotasi rahasia dibandingkan dengan frekuensi maksimum yang diizinkan. Aturannya adalah NON_COMPLIANT jika rahasia tidak dijadwalkan untuk rotasi. Aturannya juga

NON_COMPLIANT jika frekuensi rotasi lebih tinggi dari angka yang ditentukan dalam parameter Frekuensi. maximumAllowedRotation

> **Note**
>
> Mengevaluasi ulang aturan ini dalam waktu 4 jam dari evaluasi pertama tidak akan berpengaruh pada hasil.

Pengidentifikasi: SECRETSMANAGER_ROTATION_ENABLED_CHECK

Jenis Sumber Daya: AWS::SecretsManager::Secret

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Meksiko (Tengah), Asia Pasifik (Taipei)

Parameter:

maximumAllowedRotationFrekuensi (Opsional), Jenis: int

Frekuensi rotasi maksimum yang diizinkan dari rahasia dalam beberapa hari.

maximumAllowedRotationFrequencyInHours (Opsional), Jenis: int

Frekuensi rotasi maksimum yang diizinkan dari rahasia dalam jam.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

secretsmanager-scheduled-rotation-success-periksa

Memeriksa apakah AWS rahasia Secrets Manager berhasil diputar sesuai dengan jadwal rotasi. Secrets Manager menghitung tanggal rotasi harus terjadi. Aturannya adalah NON_COMPLIANT jika tanggal berlalu dan rahasianya tidak diputar.

> **Note**
>
> Penundaan perekaman

Hasil evaluasi untuk aturan ini dapat ditunda hingga 2 hari dari tanggal rotasi yang terlewat. Untuk pemantauan lebih cepat, lihat Memantau AWS Secrets Manager dengan Amazon CloudWatch di Panduan Pengguna Secrets Manager.

Rahasia tanpa rotasi

Aturan mengembalikan `NOT_APPLICABLE` rahasia yang tidak dikonfigurasi untuk rotasi.

Pengidentifikasi: SECRETSMANAGER_SCHEDULED_ROTATION_SUCCESS_CHECK

Jenis Sumber Daya: AWS::SecretsManager::Secret

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Meksiko (Tengah), Asia Pasifik (Taipei)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

secretsmanager-secret-periodic-rotation

Memeriksa apakah AWS rahasia Secrets Manager telah diputar dalam jumlah hari yang ditentukan sebelumnya. Aturannya adalah NON_COMPLIANT jika rahasia belum diputar selama lebih dari jumlah hari maxDaysSince Rotasi. Nilai default adalah 90 hari.

Pengidentifikasi: SECRETSMANAGER_SECRET_PERIODIC_ROTATION

Jenis Sumber Daya: AWS::SecretsManager::Secret

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Meksiko (Tengah), Asia Pasifik (Taipei)

Parameter:

maxDaysSinceRotasi (Opsional), Jenis: int

Jumlah hari maksimum di mana rahasia dapat tetap tidak berubah. Nilai default adalah 90 hari.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

secretsmanager-secret-unused

Memeriksa apakah AWS rahasia Secrets Manager telah diakses dalam beberapa hari tertentu. Aturannya adalah NON_COMPLIANT jika rahasia belum diakses dalam jumlah hari unusedForDays ". Nilai defaultnya adalah 90 hari.

Konteks: Disarankan untuk secara rutin menghapus rahasia yang tidak digunakan. Rahasia yang tidak digunakan dapat disalahgunakan oleh mantan pengguna yang tidak lagi membutuhkan akses ke rahasia ini. Selain itu, karena semakin banyak pengguna mendapatkan akses ke rahasia, menjadi semakin mungkin bahwa seseorang telah menyalahgunakan rahasia atau telah memberikan akses ke entitas yang tidak sah. Menghapus rahasia yang tidak digunakan membantu mencabut akses rahasia dari pengguna yang tidak lagi membutuhkannya, dan dapat mengurangi biaya penggunaan Anda. AWS Secrets Manager

Pengidentifikasi: SECRETSMANAGER_SECRET_UNUSED

Jenis Sumber Daya: AWS::SecretsManager::Secret

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Meksiko (Tengah), Asia Pasifik (Taipei)

Parameter:

unusedForDays (Opsional), Jenis: int

Jumlah hari di mana rahasia dapat tetap tidak digunakan. Nilai defaultnya adalah 90 hari.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

secretsmanager-using-cmk

Memeriksa apakah semua rahasia dienkripsi menggunakan Kunci yang dikelola AWS (`aws/secretsmanager`) atau kunci terkelola pelanggan yang dibuat di AWS Key Management Service ()AWS KMS. AWS Secrets Manager Aturannya adalah COMPLIANT jika rahasia dienkripsi menggunakan kunci yang dikelola pelanggan. Aturan ini NON_COMPLIANT jika rahasia dienkripsi menggunakan. `aws/secretsmanager`

> **Note**
>
> Aturan ini tidak memiliki akses ke kunci terkelola pelanggan lintas akun dan mengevaluasi rahasia sebagai NON_COMPLIANT saat kunci lintas akun digunakan.

Pengidentifikasi: SECRETSMANAGER_USING_CMK

Jenis Sumber Daya: AWS::SecretsManager::Secret

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei)

Parameter:

kmsKeyArns (Opsional), Jenis: CSV

Daftar dipisahkan koma dari kunci KMS Amazon Resource Names (ARNs) untuk memeriksa apakah kunci digunakan dalam enkripsi.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

Securityhub-enabled

Memeriksa apakah AWS Security Hub diaktifkan untuk AWS Akun. Aturannya adalah NON_COMPLIANT jika AWS Security Hub tidak diaktifkan.

Pengidentifikasi: SECURITYHUB_ENAB_ENABLED

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

security-account-information-provided

Memeriksa apakah Anda telah memberikan informasi kontak keamanan untuk kontak AWS akun Anda. Aturannya adalah NON_COMPLIANT jika informasi kontak keamanan dalam akun tidak disediakan.

Pengidentifikasi: SECURITY_ACCOUNT_INFORMATION_PROVIDED

Jenis Sumber Daya: AWS: :::Akun

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), AWS GovCloud (AS-Timur), AWS GovCloud (AS-Barat), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

service-catalog-shared-within-organisasi

Memeriksa apakah AWS Service Catalog membagikan portofolio ke organisasi (kumpulan AWS akun yang diperlakukan sebagai satu unit) saat integrasi diaktifkan dengan Organizations AWS . Aturannya adalah NON_COMPLIANT jika nilai `Type` dari sebuah share adalah `ACCOUNT`.

Pengidentifikasi: SERVICE_CATALOG_SHARED_WITHIN_ORGANIZATION

Jenis Sumber Daya: AWS::ServiceCatalog::Portfolio

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

service-vpc-endpoint-enabled

Memeriksa apakah Titik Akhir Layanan untuk layanan yang disediakan dalam parameter aturan dibuat untuk setiap Amazon Virtual Private Cloud (Amazon VPC). Aturannya adalah NON_COMPLIANT jika VPC Amazon tidak memiliki titik akhir VPC Amazon yang dibuat untuk layanan tersebut.

Pengidentifikasi: SERVICE_VPC_ENDPOINT_ENABLED

Jenis Sumber Daya: AWS::EC2::VPC

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

serviceName, Tipe: String

> Nama pendek atau akhiran untuk layanan. Catatan: Untuk mendapatkan daftar nama layanan yang tersedia atau daftar akhiran yang valid, gunakan DescribeVpcEndpointServices.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ses-malware-scanning-enabled

Memeriksa apakah pemindaian malware dan spam saat menerima pesan diaktifkan untuk Amazon Simple Email Service (Amazon SES). Aturannya adalah NON_COMPLIANT jika pemindaian malware dan spam tidak diaktifkan.

Pengidentifikasi: SES_MALWARE_SCANNING_ENABLED

Jenis Sumber Daya: AWS::SES::ReceiptRule

Jenis pemicu: Berkala

Wilayah AWS: Hanya tersedia di Eropa (Irlandia), Wilayah AS Timur (Virginia N.), Wilayah AS Barat (Oregon)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

shield-advanced-enabled-autorenew

Memeriksa apakah AWS Shield Advanced diaktifkan di AWS akun Anda dan langganan ini diatur untuk diperpanjang secara otomatis. Aturannya SESUAI jika Shield Advanced diaktifkan dan perpanjangan otomatis diaktifkan.

> **Note**
>
> Titik akhir API hanya AWS Shield Advanced tersedia di Wilayah AS Timur (Virginia N.). Aturan ini seharusnya hanya dijadwalkan untuk berjalan di Wilayah AS Timur (Virginia N.).

Pengidentifikasi: SHIELD_ADVANCED_ENABLED_AUTORENEW

Jenis pemicu: Berkala

Wilayah AWS: Hanya tersedia di Wilayah AS Timur (Virginia Utara)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

shield-drt-access

Memeriksa apakah Tim Respons Shield (SRT) dapat mengakses AWS akun Anda. Aturannya adalah NON_COMPLIANT jika AWS Shield Advanced diaktifkan tetapi peran untuk akses SRT tidak dikonfigurasi.

Pengidentifikasi: SHIELD_DRT_ACCESS

Jenis pemicu: Berkala

Wilayah AWS: Hanya tersedia di Wilayah AS Timur (Virginia Utara)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

sns-encrypted-kms

Memeriksa apakah topik SNS dienkripsi dengan AWS Key Management Service (AWS KMS). Aturannya adalah NON_COMPLIANT jika topik SNS tidak dienkripsi dengan KMS. AWS Secara opsional, tentukan kunci ARNs, alias ARNs, nama alias, atau kunci IDs untuk diperiksa aturan.

Pengidentifikasi: SNS_ENCRYPTED_KMS

Jenis Sumber Daya: AWS::SNS::Topic

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

kmsKeyIds (Opsional), Jenis: CSV

> Daftar AWS kunci KMS yang dipisahkan koma Nama Sumber Daya Amazon (ARNs), alias KMS, nama alias KMS ARNs, atau kunci KMS untuk diperiksa aturan. IDs

Evaluasi Proaktif

Untuk langkah-langkah tentang cara menjalankan aturan ini dalam mode proaktif, lihat Mengevaluasi Sumber Daya Anda dengan AWS Config Aturan. Agar aturan ini mengembalikan COMPLIANT dalam mode proaktif, skema konfigurasi sumber daya untuk StartResourceEvaluationAPI harus menyertakan input berikut, yang dikodekan sebagai string:

```
"ResourceConfiguration":
...
{
   "KmsMasterKeyId": "my-kms-key-Id"
}
...
```

Untuk informasi lebih lanjut tentang evaluasi proaktif, lihat Mode Evaluasi.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

sns-topic-message-delivery-notifikasi-diaktifkan

Memeriksa apakah pencatatan Amazon Simple Notification Service (SNS) diaktifkan untuk status pengiriman pesan notifikasi yang dikirim ke topik untuk titik akhir. Aturannya adalah NON_COMPLIANT jika pemberitahuan status pengiriman untuk pesan tidak diaktifkan.

Pengidentifikasi: SNS_TOPIC_MESSAGE_DELIVERY_NOTIFICATION_ENABLED

Jenis Sumber Daya: AWS::SNS::Topic

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur), AWS GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

sns-topic-no-public-akses

Memeriksa apakah kebijakan akses topik SNS mengizinkan akses publik. Aturannya adalah NON_COMPLIANT jika kebijakan akses topik SNS mengizinkan akses publik.

> **Note**
>
> Agar dianggap non-publik, kebijakan SNS harus memberikan akses hanya ke nilai tetap. Ini berarti nilai yang tidak mengandung wildcard atau elemen kebijakan IAM berikut: Variabel.

Pengidentifikasi: SNS_TOPIC_NO_PUBLIC_ACCESS

Jenis Sumber Daya: AWS::SNS::Topic

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), AWS GovCloud (AS-Timur), AWS GovCloud (AS-Barat), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

sqs-queue-no-public-akses

Memeriksa apakah kebijakan akses antrian SQS memungkinkan akses publik. Aturannya adalah NON_COMPLIANT jika kebijakan akses antrian SQS mengizinkan akses publik.

> **Note**
>
> Agar dianggap non-publik, kebijakan SQS harus memberikan akses hanya ke nilai tetap. Ini berarti nilai yang tidak mengandung wildcard atau elemen kebijakan IAM berikut: Variabel.

Pengidentifikasi: SQS_QUEUE_NO_PUBLIC_ACCESS

Jenis Sumber Daya: AWS::SQS::Queue

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (Bahrain), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur), AWS GovCloud (AWS GovCloud AS-Barat), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ssm-automation-block-public-berbagi

Memeriksa apakah AWS Systems Manager Automation telah memblokir berbagi publik yang diaktifkan. Aturannya adalah NON_COMPLIANT jika Systems Manager Automation telah memblokir berbagi publik dinonaktifkan.

Pengidentifikasi: SSM_AUTOMATION_BLOCK_PUBLIC_SHARING

Jenis Sumber Daya: AWS: :::Akun

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Seoul), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

ssm-automation-logging-enabled

Memeriksa apakah AWS Systems Manager Automation mengaktifkan CloudWatch pencatatan Amazon. Aturan mengembalikan NON_COMPLIANT jika Systems Manager Automation tidak mengaktifkan logging. CloudWatch

Pengidentifikasi: SSM_AUTOMATION_LOGGING_ENABLED

Jenis Sumber Daya: AWS: :::Akun

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Seoul), Asia Pasifik (Malaysia), Meksiko (Tengah),

Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ssm-document-not-public

Memeriksa apakah dokumen AWS Systems Manager yang dimiliki oleh akun bersifat publik. Aturannya adalah NON_COMPLIANT jika dokumen Systems Manager dengan pemilik 'Self' bersifat publik.

Pengidentifikasi: SSM_DOCUMENT_NOT_PUBLIC

Jenis Sumber Daya: AWS::SSM::Document

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Taipei), Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

ssm-document-tagged

Memeriksa apakah dokumen AWS Systems Manager memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: SSM_DOCUMENT_TAGGED

Jenis Sumber Daya: AWS::SSM::Document

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

step-functions-state-machine-logging-diaktifkan

Memeriksa apakah mesin AWS Step Functions telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika mesin status tidak mengaktifkan logging atau konfigurasi logging tidak pada tingkat minimum yang disediakan.

Pengidentifikasi: STEP_FUNCTIONS_STATE_MACHINE_LOGGING_ENABLED

Jenis Sumber Daya: AWS::StepFunctions::StateMachine

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur), AWS GovCloud (AS-Barat), Meksiko AWS GovCloud (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary) Wilayah

Parameter:

cloudWatchLogGroupArns (Opsional), Jenis: CSV

Daftar Nama Sumber Daya Amazon (ARNs) yang dipisahkan koma untuk grup CloudWatch log Amazon Logs. Aturan memeriksa apakah grup log yang ditentukan dikonfigurasi untuk log mesin status Anda.

LogLevel (Opsional), Tipe: String

Tingkat log minimum untuk mesin negara Anda. Nilai yang valid meliputi: ALL, ERROR, FATAL.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

storagegateway-last-backup-recovery-point-dibuat

Memeriksa apakah titik pemulihan dibuat untuk volume AWS Storage Gateway. Aturannya adalah NON_COMPLIANT jika volume Storage Gateway tidak memiliki titik pemulihan yang sesuai yang dibuat dalam periode waktu yang ditentukan.

Pengidentifikasi: STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED

Jenis Sumber Daya: AWS::StorageGateway::Volume

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

ResourceTags (Opsional), Tipe: String

Tag volume Storage Gateway untuk aturan yang akan diperiksa, dalam format `{"tagkey" : "tagValue"}` JSON.

ResourceID (Opsional), Tipe: String

ID volume Storage Gateway untuk aturan yang akan diperiksa.

recoveryPointAgeNilai (Opsional), Jenis: int, Default: 1

Nilai numerik untuk usia maksimum yang diizinkan. Tidak lebih dari 744 jam, 31 untuk hari.

recoveryPointAgeUnit (Opsional), Tipe: String, Default: hari

Satuan waktu untuk usia maksimum yang diizinkan. Nilai yang diterima: 'jam', 'hari'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

storagegateway-resources-in-logically-air-gapped-vault

Memeriksa apakah volume AWS Storage Gateway berada dalam brankas yang memiliki gap udara secara logis. Aturannya adalah NON_COMPLIANT jika volume AWS Storage Gateway tidak berada dalam vault yang memiliki gapped udara secara logis dalam periode waktu yang ditentukan.

Pengidentifikasi: STORAGEGATEWAY_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

Jenis Sumber Daya: AWS::StorageGateway::Volume

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

ResourceTags (Opsional), Tipe: String

Tag volume Storage Gateway untuk aturan yang akan diperiksa, dalam format JSON.

ResourceID (Opsional), Tipe: String

ID volume Storage Gateway untuk diperiksa aturan.

recoveryPointAgeNilai (Opsional), Jenis: int, Default: 1

Nilai numerik untuk usia maksimum yang diizinkan. Tidak lebih dari 2184 jam, 91 untuk hari.

recoveryPointAgeUnit (Opsional), Tipe: String, Default: hari

Satuan waktu untuk usia maksimum yang diizinkan. Nilai yang diterima: 'jam', 'hari'.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

storagegateway-resources-protected-by-rencana cadangan

Memeriksa apakah volume AWS Storage Gateway dilindungi oleh paket cadangan. Aturannya adalah NON_COMPLIANT jika volume Storage Gateway tidak dicakup oleh rencana cadangan.

Pengidentifikasi: STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Jenis Sumber Daya: AWS::StorageGateway::Volume

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

ResourceTags (Opsional), Tipe: String

Tag untuk Volume Gateway Storage untuk aturan yang akan diperiksa, dalam format JSON.

ResourceID (Opsional), Tipe: String

ID volume Storage Gateway untuk diperiksa aturan.

crossRegionList (Opsional), Tipe: String

Daftar wilayah tujuan yang dipisahkan koma untuk salinan cadangan lintas wilayah yang akan disimpan

crossAccountList (Opsional), Tipe: String

Daftar akun tujuan yang dipisahkan koma untuk salinan cadangan lintas akun yang akan disimpan

maxRetentionDays (Opsional), Jenis: int

Periode retensi maksimum dalam beberapa hari untuk Backup Vault Lock

minRetentionDays (Opsional), Jenis: int

Periode retensi minimum dalam beberapa hari untuk Backup Vault Lock

backupVaultLockPeriksa (Opsional), Tipe: String

Nilai yang diterima: 'Benar' atau 'False'. Masukkan 'Benar' untuk aturan untuk memeriksa apakah sumber daya dicadangkan di brankas yang terkunci

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

subnet-auto-assign-public-ip-dinonaktifkan

Memeriksa apakah subnet Amazon Virtual Private Cloud (Amazon VPC) diberi alamat IP publik. Aturannya SESUAI jika Amazon VPC tidak memiliki subnet yang diberi alamat IP publik. Aturannya adalah NON_COMPLIANT jika Amazon VPC memiliki subnet yang diberi alamat IP publik.

Pengidentifikasi: SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED

Jenis Sumber Daya: AWS::EC2::Subnet

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

Tidak ada

Evaluasi Proaktif

Untuk langkah-langkah tentang cara menjalankan aturan ini dalam mode proaktif, lihat Mengevaluasi Sumber Daya Anda dengan AWS Config Aturan. Agar aturan ini mengembalikan COMPLIANT dalam mode proaktif, skema konfigurasi sumber daya untuk StartResourceEvaluationAPI harus menyertakan input berikut, yang dikodekan sebagai string:

```
"ResourceConfiguration":
...
{
   "MapPublicIpOnLaunch": BOOLEAN
}
...
```

Untuk informasi lebih lanjut tentang evaluasi proaktif, lihat Mode Evaluasi.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

transfer-agreement-description

Memeriksa apakah perjanjian AWS Transfer Family memiliki deskripsi. Aturannya adalah NON_COMPLIANT jika Configuration.description tidak ada.

Pengidentifikasi: TRANSFER_AGREEMENT_DESCRIPTION

Jenis Sumber Daya: AWS::Transfer::Agreement

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningbo Xia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

transfer-agreement-tagged

Memeriksa apakah perjanjian AWS Transfer Family memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: TRANSFER_AGREEMENT_TAGGED

Jenis Sumber Daya: AWS::Transfer::Agreement

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningbo Xia), Wilayah Eropa (Zurich)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

transfer-certificate-description

Memeriksa apakah sertifikat AWS Transfer Family memiliki deskripsi. Aturannya adalah NON_COMPLIANT jika Configuration.description tidak ada.

Pengidentifikasi: TRANSFER_CERTIFICATE_DESCRIPTION

Jenis Sumber Daya: AWS::Transfer::Certificate

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

transfer-certificate-tagged

Memeriksa apakah sertifikat AWS Transfer Family memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: TRANSFER_CERTIFICATE_TAGGED

Jenis Sumber Daya: AWS::Transfer::Certificate

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

transfer-connector-logging-enabled

Memeriksa apakah AWS Transfer Family Connector menerbitkan log ke Amazon CloudWatch. Aturannya adalah NON_COMPLIANT jika Konektor tidak memiliki yang ditetapkan. LoggingRole

Pengidentifikasi: TRANSFER_CONNECTOR_LOGGING_ENABLED

Jenis Sumber Daya: AWS::Transfer::Connector

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (Bahrain), Asia Pasifik (Thailand), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko

(Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

transfer-connector-tagged

Memeriksa apakah konektor AWS Transfer Family memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: TRANSFER_CONNECTOR_TAGGED

Jenis Sumber Daya: AWS::Transfer::Connector

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

transfer-family-server-no-ftp

Memeriksa apakah server yang dibuat dengan AWS Transfer Family menggunakan FTP untuk koneksi endpoint. Aturannya adalah NON_COMPLIANT jika protokol server untuk koneksi endpoint diaktifkan FTP.

Pengidentifikasi: TRANSFER_FAMILY_SERVER_NO_FTP

Jenis Sumber Daya: AWS::Transfer::Server

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

transfer-profile-tagged

Memeriksa apakah profil AWS Transfer Family memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: TRANSFER_PROFILE_TAGGED

Jenis Sumber Daya: AWS::Transfer::Profile

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

transfer-workflow-description

Memeriksa apakah alur kerja AWS Transfer Family memiliki deskripsi. Aturannya adalah NON_COMPLIANT jika Configuration.description tidak ada atau string kosong.

Pengidentifikasi: TRANSFER_WORKFLOW_DESCRIPTION

Jenis Sumber Daya: AWS::Transfer::Workflow

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

transfer-workflow-tagged

Memeriksa apakah alur kerja AWS Transfer Family memiliki tag. Secara opsional, Anda dapat menentukan kunci tag. Aturannya adalah NON_COMPLIANT jika tidak ada tag atau jika kunci tag yang ditentukan tidak ada. Aturan tidak memeriksa tag yang dimulai dengan 'aws: '.

Pengidentifikasi: TRANSFER_WORKFLOW_TAGGED

Jenis Sumber Daya: AWS::Transfer::Workflow

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Tiongkok (Ningxia)

Parameter:

requiredKeyTags (Opsional), Jenis: CSV

> Daftar kunci tag yang dipisahkan koma untuk diperiksa aturan. Jika disediakan, aturannya adalah NON_COMPLIANT jika sumber daya yang dievaluasi tidak berisi kunci ini. Kunci tag peka terhadap huruf besar dan kecil. Tombol tag yang dimulai dengan 'aws: 'tidak diperbolehkan.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

virtualmachine-last-backup-recovery-point-dibuat

Memeriksa apakah titik pemulihan dibuat untuk AWS VirtualMachines Backup-Gateway. Aturannya adalah NON_COMPLIANT jika AWS Backup-Gateway VirtualMachines tidak memiliki titik pemulihan yang sesuai yang dibuat dalam periode waktu yang ditentukan.

Pengidentifikasi: VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED

Jenis Sumber Daya: AWS::BackupGateway::VirtualMachine

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

ResourceTags (Opsional), Tipe: String

Tag AWS Backup-Gateway VirtualMachines untuk aturan yang akan diperiksa, dalam format JSON. `{"tagkey" : "tagValue"}`

ResourceID (Opsional), Tipe: String

ID AWS Backup-Gateway VirtualMachine untuk aturan yang akan diperiksa.

recoveryPointAgeNilai (Opsional), Jenis: int, Default: 1

Nilai numerik untuk usia maksimum yang diizinkan. Tidak lebih dari 744 jam, 31 untuk hari.

recoveryPointAgeUnit (Opsional), Tipe: String, Default: hari

Satuan waktu untuk usia maksimum yang diizinkan. Nilai yang diterima: 'jam', 'hari'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

virtualmachine-resources-in-logically-air-gapped-vault

Memeriksa apakah AWS Backup-Gateway VirtualMachines berada dalam brankas yang memiliki lubang udara secara logis. Aturannya adalah NON_COMPLIANT jika AWS Backup-Gateway tidak VirtualMachines berada dalam brankas dengan lubang udara secara logis dalam periode waktu yang ditentukan.

Pengidentifikasi: VIRTUALMACHINE_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

Jenis Sumber Daya: AWS::BackupGateway::VirtualMachine

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

ResourceTags (Opsional), Tipe: String

Tag AWS Backup-Gateway VirtualMachines untuk aturan yang akan diperiksa, dalam format JSON.

ResourceID (Opsional), Tipe: String

ID AWS Backup-Gateway VirtualMachine untuk aturan yang akan diperiksa.

recoveryPointAgeNilai (Opsional), Jenis: int, Default: 1

Nilai numerik untuk usia maksimum yang diizinkan. Tidak lebih dari 2184 jam, 91 untuk hari.

recoveryPointAgeUnit (Opsional), Tipe: String, Default: hari

Satuan waktu untuk usia maksimum yang diizinkan. Nilai yang diterima: 'jam', 'hari'.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

virtualmachine-resources-protected-by-rencana cadangan

Memeriksa apakah AWS Backup-Gateway VirtualMachines dilindungi oleh paket cadangan. Aturannya adalah NON_COMPLIANT jika Backup-Gateway tidak dicakup VirtualMachine oleh rencana cadangan.

Pengidentifikasi: VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Jenis Sumber Daya: AWS::BackupGateway::VirtualMachine

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

ResourceTags (Opsional), Tipe: String

Tag untuk AWS Backup-Gateway VirtualMachines untuk aturan yang akan diperiksa, dalam format JSON. `{"tagkey" : "tagValue"}`

ResourceID (Opsional), Tipe: String

ID AWS Backup-Gateway VirtualMachine untuk aturan yang akan diperiksa.

crossRegionList (Opsional), Tipe: String

Daftar wilayah tujuan yang dipisahkan koma untuk salinan cadangan lintas wilayah yang akan disimpan

crossAccountList (Opsional), Tipe: String

Daftar akun tujuan yang dipisahkan koma untuk salinan cadangan lintas akun yang akan disimpan

maxRetentionDays (Opsional), Jenis: int

Periode retensi maksimum dalam beberapa hari untuk Backup Vault Lock

minRetentionDays (Opsional), Jenis: int

Periode retensi minimum dalam beberapa hari untuk Backup Vault Lock

backupVaultLockPeriksa (Opsional), Tipe: String

Nilai yang diterima: 'Benar' atau 'False'. Masukkan 'Benar' untuk aturan untuk memeriksa apakah sumber daya dicadangkan di brankas yang terkunci

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

vpc-default-security-group-tertutup

Memeriksa apakah grup keamanan default Amazon Virtual Private Cloud (Amazon VPC) tidak mengizinkan lalu lintas masuk atau keluar. Aturannya adalah NON_COMPLIANT jika grup keamanan default memiliki satu atau lebih aturan lalu lintas masuk atau keluar.

> **Note**
>
> Mungkin ada penundaan antara saat AWS Config mencatat penghapusan sumber daya terkait seperti grup keamanan default, yang dihapus sebagai bagian dari penghapusan VPC Amazon. Akibatnya, meskipun semua grup keamanan default atau sumber daya terkait lainnya telah dihapus atau diperbaiki, aturan dapat melaporkan NON_COMPLIANT hingga proses baselining akun berikutnya.

Pengidentifikasi: VPC_DEFAULT_SECURITY_GROUP_CLOSED

Jenis Sumber Daya: AWS::EC2::SecurityGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

vpc-endpoint-enabled

Memeriksa apakah setiap layanan yang ditentukan dalam parameter memiliki titik akhir Amazon VPC. Aturannya adalah NON_COMPLIANT jika Amazon VPC tidak memiliki titik akhir VPC yang dibuat untuk setiap layanan yang ditentukan. Secara opsional, Anda dapat menentukan aturan tertentu VPCs untuk diperiksa.

Pengidentifikasi: VPC_ENDPOINT_ENABLED

Jenis Sumber Daya: AWS::EC2::VPC

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

ServiceNames, Jenis: CSV

> Daftar nama layanan atau titik akhir yang dipisahkan koma. Contoh: “access-analyzer, appconfig, cloudtrail” atau “com.amazonaws.region.access-analyzer”. Gunakan DescribeVpcEndpointServices untuk nama yang tersedia.

VPCIDS (Opsional), Jenis: CSV

Daftar VPC Amazon yang dipisahkan koma IDs untuk titik akhir VPC. Jika disediakan, aturannya adalah NON_COMPLIANT jika layanan yang ditentukan dalam parameter ServiceName tidak memiliki salah satu titik akhir VPC ini.

scopeConfigResourceJenis (Opsional), Jenis: CSV

Daftar tipe sumber daya AWS Config yang dipisahkan koma untuk diperiksa oleh aturan. Jika ditentukan, aturan mengembalikan status kepatuhan hanya jika setidaknya satu sumber daya yang ditentukan dicatat dalam akun. Misalnya: "AWS::SNS::Topic”.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

vpc-flow-logs-enabled

Memeriksa apakah log aliran Amazon Virtual Private Cloud (Amazon VPC) ditemukan dan diaktifkan untuk semua Amazon. VPCs Aturannya adalah NON_COMPLIANT jika log aliran tidak diaktifkan untuk setidaknya satu VPC Amazon.

Pengidentifikasi: VPC_FLOW_LOGS_ENABLED

Jenis Sumber Daya: AWS::EC2::VPC

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

TrafficType (Opsional), Tipe: String

TrafficType dari log aliran

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

vpc-network-acl-unused-periksa

Memeriksa apakah ada daftar kontrol akses jaringan yang tidak digunakan (jaringan ACLs). Aturannya adalah COMPLIANT jika setiap jaringan ACL dikaitkan dengan subnet. Aturannya adalah NON_COMPLIANT jika ACL jaringan tidak terkait dengan subnet.

Pengidentifikasi: VPC_NETWORK_ACL_UNUSED_CHECK

Jenis Sumber Daya: AWS::EC2::NetworkAcl

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

vpc-peering-dns-resolution-periksa

Memeriksa apakah resolusi DNS dari accepter/requester VPC ke IP pribadi diaktifkan. Aturannya adalah NON_COMPLIANT jika resolusi DNS dari accepter/requester VPC ke IP pribadi tidak diaktifkan.

Pengidentifikasi: VPC_PEERING_DNS_RESOLUTION_CHECK

Jenis Sumber Daya: AWS::EC2::VPCPeeringConnection

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

VPCIDS (Opsional), Jenis: CSV

Daftar VPC IDs yang dipisahkan koma untuk diperiksa.

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

vpc-sg-open-only-to-authorized-ports

Memeriksa apakah grup keamanan mengizinkan lalu lintas masuk yang tidak dibatasi ('0.0.0.0/0' atau ': :/0') hanya mengizinkan koneksi TCP atau UDP masuk pada port resmi. Aturannya adalah NON_COMPLIANT jika grup keamanan tersebut tidak memiliki port yang ditentukan dalam parameter aturan.

> **Note**
>
> Aturan ini mengevaluasi grup EC2 keamanan Amazon dengan aturan masuk yang disetel ke IPv4 ='0.0.0.0/0' atau ': :/'. IPv6 Jika grup keamanan tidak memiliki salah satu tujuan tersebut, aturan ini kembali`NOT_APPLICABLE`.

Pengidentifikasi: VPC_SG_OPEN_ONLY_TO_AUTHORIZED_PORTS

Jenis Sumber Daya: AWS::EC2::SecurityGroup

Jenis pemicu: Perubahan konfigurasi dan Periodik

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Wilayah Asia Pasifik (Melbourne)

Parameter:

authorizedTcpPorts (Opsional), Tipe: String

Daftar port TCP yang dipisahkan koma diizinkan untuk terbuka ke 0.0.0.0/0 atau: :/0. Rentang ditentukan oleh tanda hubung, misalnya, “443,1020-1025".

authorizedUdpPorts (Opsional), Tipe: String

Daftar port UDP yang dipisahkan koma diizinkan untuk terbuka ke 0.0.0.0/0 atau: :/0. Rentang ditentukan oleh tanda hubung, misalnya, “500,1020-1025".

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

vpc-sg-port-restriction-periksa

Memeriksa apakah grup keamanan membatasi lalu lintas masuk ke port terbatas secara eksplisit dari 0.0.0.0/0 atau: :/0. Aturannya adalah NON_COMPLIANT jika grup keamanan mengizinkan lalu lintas masuk dari 0.0.0.0/0 atau: :/0 melalui port 22/3389 atau seperti yang ditentukan dalam parameter. TCP/UDP

Pengidentifikasi: VPC_SG_PORT_RESTRICTION_CHECK

Jenis Sumber Daya: AWS::EC2::SecurityGroup

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Malaysia), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

RestrictPorts (Opsional), Jenis: CSV

Daftar port yang dipisahkan koma yang seharusnya tidak terbuka untuk lalu lintas masuk melalui rentang IP penuh. Nomor port yang valid berkisar dari 0 hingga 65535. Jika tidak ditentukan, aturan default untuk memeriksa 22 dan 3389.

ProtocolType (Opsional), Tipe: String

Jenis Protokol Transmisi untuk aturan yang akan diperiksa. Nilai yang valid termasuk 'TCP', 'UDP', dan 'ALL' (case-insensitive). Jika disetel ke 'ALL', aturan akan memeriksa aturan yang menggunakan protokol 'TCP', 'UDP', atau 'ALL' (-1). Nilai default adalah 'SEMUA'.

excludeExternalSecurityGrup (Opsional), Jenis: boolean

Bendera Boolean untuk mengecualikan evaluasi grup keamanan eksternal. Jika disetel ke 'true', aturan tidak akan menyertakan grup keamanan eksternal dalam evaluasi. Jika tidak, semua grup keamanan dievaluasi jika nilai disetel ke 'false.' Nilai default adalah 'benar'.

IPType (Opsional), Tipe: String

Versi Internet Protocol (IP) untuk aturan yang akan diperiksa. Nilai yang valid termasuk 'IPv4', 'IPv6', dan 'SEMUA' (case-insensitive). Jika tidak ditentukan, aturan default untuk memeriksa 'SEMUA'.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

vpc-vpn-2-terowongan

Memeriksa apakah kedua terowongan jaringan pribadi virtual (VPN) yang disediakan oleh AWS Site-to-Site VPN berada dalam status UP. Aturannya adalah NON_COMPLIANT jika salah satu atau kedua terowongan berada dalam status DOWN.

Pengidentifikasi: VPC_VPN_2_TUNNELS_UP

Jenis Sumber Daya: AWS::EC2::VPNConnection

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Timur Tengah (Bahrain), Tiongkok (Beijing), Asia Pasifik (Osaka), Israel (Tel Aviv), Wilayah Tiongkok (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

wafv2-logging diaktifkan

Memeriksa apakah pencatatan diaktifkan pada daftar kontrol akses web AWS WAFv2 regional dan global (web ACLs). Aturannya adalah NON_COMPLIANT jika logging diaktifkan tetapi tujuan logging tidak cocok dengan nilai parameter.

> **Note**
>
> Pengecualian Danau Keamanan Amazon
> Aturan ini tidak memeriksa pencatatan yang dilakukan dengan Security Lake untuk AWS WAFV2 web ACLs.

Pengidentifikasi: _LOGGING_ENABLED WAFV2

Jenis Sumber Daya: AWS::WAFv2::WebACL

Jenis pemicu: Berkala

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Meksiko (Tengah), Wilayah Asia Pasifik (Taipei)

Parameter:

KinesisFirehoseDeliveryStreamArns (Opsional), Jenis: CSV

Daftar aliran pengiriman Kinesis Firehose yang dipisahkan koma ARNs

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

wafv2- rulegroup-logging-enabled

Memeriksa apakah pengumpulan metrik CloudWatch keamanan Amazon pada grup AWS WAFv2 aturan diaktifkan. Aturannya adalah NON_COMPLIANT jika '. VisibilityConfig CloudWatchMetricsEnabled'bidang disetel ke false.

Konteks: AWS WAFV2 (Web Application Firewall versi 2) memungkinkan Anda membuat AWS WAF aturan untuk melindungi aplikasi web Anda dari eksploitasi dan kerentanan web umum. Grup AWS WAF aturan adalah kumpulan AWS WAF aturan yang dapat Anda kaitkan dengan ACL web (Access Control List) untuk menentukan perilaku yang diinginkan untuk lalu lintas aplikasi web Anda. Untuk informasi selengkapnya, lihat AWS WAF aturan dan Grup aturan di Panduan AWS WAF Pengembang.

Dengan mengonfigurasi pengumpulan metrik CloudWatch keamanan pada grup AWS WAFV2 aturan, Anda dapat memantau metrik keamanan seperti serangan Distributed denial of service (DDoS), SQL injection, dan cross-site scripting (XSS) yang berhasil atau gagal. Metrik keamanan yang dikumpulkan dapat membantu Anda menyederhanakan penyelidikan.

> **Note**
>
> Jika tidak ada AWS WAF aturan dalam grup AWS WAFV2 aturan untuk diperiksa oleh aturan AWS Config terkelola, aturan AWS Config terkelola akan kembali`NOT_APPLICABLE`.

Pengidentifikasi: _RULEGROUP_LOGGING_ENABLED WAFV2

Jenis Sumber Daya: AWS::WAFv2::RuleGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), AWS GovCloud (AS-Timur), AWS GovCloud (AS-Barat), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

wafv2- rulegroup-not-empty

Memeriksa apakah Grup WAFv2 Aturan berisi aturan. Aturannya adalah NON_COMPLIANT jika tidak ada aturan dalam Grup Aturan. WAFv2

Pengidentifikasi: _RULEGROUP_NOT_EMPTY WAFV2

Jenis Sumber Daya: AWS::WAFv2::RuleGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), Asia Pasifik (Melbourne), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

wafv2- webacl-not-empty

Memeriksa apakah ACL WAFv2 Web berisi aturan WAF atau grup aturan WAF. Aturan ini NON_COMPLIANT jika ACL Web tidak berisi aturan WAF atau grup aturan WAF.

Pengidentifikasi: _WEBACL_NOT_EMPTY WAFV2

Jenis Sumber Daya: AWS::WAFv2::WebACL

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Malaysia), AWS GovCloud (AS-Timur), (AS-Barat), Meksiko AWS GovCloud (Tengah), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

waf-classic-logging-enabled

Memeriksa apakah pencatatan diaktifkan pada daftar kontrol akses web global klasik AWS WAF (web ACLs). Aturannya adalah NON_COMPLIANT untuk ACL web global, jika tidak mengaktifkan logging.

Pengidentifikasi: WAF_CLASSIC_LOGGING_ENABLED

Jenis Sumber Daya: AWS::WAF::WebACL

Jenis pemicu: Berkala

Wilayah AWS: Hanya tersedia di Wilayah AS Timur (Virginia Utara)

Parameter:

KinesisFirehoseDeliveryStreamArns (Opsional), Jenis: CSV

Daftar AWS ARN aliran Amazon Kinesis yang dipisahkan koma untuk log WAF.

AWS CloudFormation template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

waf-global-rulegroup-not-kosong

Memeriksa apakah grup aturan AWS WAF Classic berisi aturan apa pun. Aturannya adalah NON_COMPLIANT jika tidak ada aturan yang ada dalam grup aturan.

Pengidentifikasi: WAF_GLOBAL_RULEGROUP_NOT_EMPTY

Jenis Sumber Daya: AWS::WAF::RuleGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Wilayah AS Timur (Virginia Utara)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

waf-global-rule-not-kosong

Memeriksa apakah aturan global AWS WAF berisi kondisi apa pun. Aturannya adalah NON_COMPLIANT jika tidak ada kondisi dalam aturan global WAF.

Pengidentifikasi: WAF_GLOBAL_RULE_NOT_EMPTY

Jenis Sumber Daya: AWS::WAF::Rule

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Wilayah AS Timur (Virginia Utara)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

waf-global-webacl-not-kosong

Memeriksa apakah WAF Global Web ACL berisi aturan WAF atau grup aturan. Aturan ini adalah NON_COMPLIANT jika ACL Web tidak berisi aturan WAF atau grup aturan.

Pengidentifikasi: WAF_GLOBAL_WEBACL_NOT_EMPTY

Jenis Sumber Daya: AWS::WAF::WebACL

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Wilayah AS Timur (Virginia Utara)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

waf-regional-rulegroup-not-kosong

Memeriksa apakah kelompok aturan WAF Regional berisi aturan apa pun. Aturannya adalah NON_COMPLIANT jika tidak ada aturan yang ada dalam grup aturan Regional WAF.

Pengidentifikasi: WAF_REGIONAL_RULEGROUP_NOT_EMPTY

Jenis Sumber Daya: AWS::WAFRegional::RuleGroup

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali China (Beijing), Asia Pasifik (Thailand), Asia Pasifik (Jakarta), Timur Tengah (UEA), Asia Pasifik (Hyderabad), Asia Pasifik (Osaka), Asia Pasifik (Malaysia), (AS-Timur) AWS GovCloud , (AS-Barat) AWS GovCloud , Meksiko (Tengah), Israel (Tel Aviv), Asia Pasifik (Taipei), Kanada Barat (Calgary), Eropa (Spanyol), Tiongkok (Ningxia), Wilayah Eropa (Zurich)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

waf-regional-rule-not-kosong

Memeriksa apakah aturan regional WAF berisi kondisi. Aturan ini COMPLIANT jika aturan regional berisi setidaknya satu kondisi dan NON_COMPLIANT sebaliknya.

Pengidentifikasi: WAF_REGIONAL_RULE_NOT_EMPTY

Jenis Sumber Daya: AWS::WAFRegional::Rule

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), AWS GovCloud (AS-Timur), AWS GovCloud (AS-Barat), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

waf-regional-webacl-not-kosong

Memeriksa apakah ACL Web regional WAF berisi aturan WAF atau grup aturan. Aturannya adalah NON_COMPLIANT jika tidak ada aturan WAF atau grup aturan yang ada dalam ACL Web.

Pengidentifikasi: WAF_REGIONAL_WEBACL_NOT_EMPTY

Jenis Sumber Daya: AWS::WAFRegional::WebACL

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Semua AWS wilayah yang didukung kecuali Asia Pasifik (Thailand), Asia Pasifik (Malaysia), AWS GovCloud (AS-Timur), AWS GovCloud (AS-Barat), Meksiko (Tengah), Asia Pasifik (Taipei), Wilayah Kanada Barat (Calgary)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

workspaces-root-volume-encryption-diaktifkan

Memeriksa apakah WorkSpace volume Amazon memiliki pengaturan enkripsi volume root yang disetel ke diaktifkan. Aturan ini adalah NON_COMPLIANT jika pengaturan enkripsi tidak diaktifkan untuk volume root.

Pengidentifikasi: WORKSPACES_ROOT_VOLUME_ENCRYPTION_ENABLED

Jenis Sumber Daya: AWS::WorkSpaces::Workspace

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Asia Pasifik (Mumbai), Afrika (Cape Town), Eropa (Irlandia), Eropa (Frankfurt), Amerika Selatan (Sao Paulo), AS Timur (Virginia N.), Asia Pasifik (Seoul), Eropa (London), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Kanada (Tengah), China Wilayah (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihat[Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template](#).

workspaces-user-volume-encryption-diaktifkan

Memeriksa apakah WorkSpace volume Amazon memiliki pengaturan enkripsi volume pengguna yang disetel ke diaktifkan. Aturan ini adalah NON_COMPLIANT jika pengaturan enkripsi tidak diaktifkan untuk volume pengguna.

Pengidentifikasi: WORKSPACES_USER_VOLUME_ENCRYPTION_ENABLED

Jenis Sumber Daya: AWS::WorkSpaces::Workspace

Jenis pemicu: Perubahan konfigurasi

Wilayah AWS: Hanya tersedia di Asia Pasifik (Mumbai), Afrika (Cape Town), Eropa (Irlandia), Eropa (Frankfurt), Amerika Selatan (Sao Paulo), AS Timur (Virginia N.), Asia Pasifik (Seoul), Eropa

(London), Asia Pasifik (Tokyo), AS Barat (Oregon), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Kanada (Tengah), China Wilayah (Ningxia)

Parameter:

Tidak ada

AWS CloudFormation Template

Untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation templat, lihatMembuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.

Daftar Aturan AWS Config Terkelola berdasarkan Mode Evaluasi

AWS Config saat ini mendukung aturan terkelola berikut. Sebelum menggunakan aturan ini, lihatPertimbangan.

Evaluasi Proaktif

Aturan proaktif adalah aturan yang mendukung mode evaluasi proaktif untuk sumber daya yang belum digunakan. Ini memungkinkan Anda untuk mengevaluasi apakah satu set properti sumber daya, jika digunakan untuk mendefinisikan AWS sumber daya, akan COMPLIANT atau NON_COMPLIANT mengingat seperangkat aturan proaktif yang Anda miliki di akun Anda di Wilayah Anda. Untuk informasi selengkapnya, lihat Mode evaluasi.

> **Note**
>
> Aturan proaktif tidak memulihkan sumber daya yang ditandai sebagai NON_COMPLIANT atau mencegahnya diterapkan.

Evaluasi Proaktif

- api-gw-xray-enabled
- autoscaling-group-elb-healthcheck-diperlukan
- ec2- instance-multiple-eni-check
- terlampir eip
- elasticsearch-node-to-node-pemeriksaan enkripsi-

- lambda-function-settings-check
- lambda-inside-vpc
- rds-automatic-minor-version-upgrade diaktifkan
- rds-enhanced-monitoring-enabled
- rds-instance-public-access-periksa
- rds-multi-az-support
- rds-storage-encrypted
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-periksa
- s3- bucket-logging-enabled
- sns-encrypted-kms
- subnet-auto-assign-public-ip-dinonaktifkan

Evaluasi Detektif

Aturan Detektif adalah aturan yang mendukung mode evaluasi detektif untuk sumber daya yang telah digunakan. Ini memungkinkan Anda untuk mengevaluasi pengaturan konfigurasi sumber daya yang ada.

> **Note**
>
> Saat ini, semua AWS Config aturan mendukung evaluasi detektif.

Evaluasi Detektif

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan

- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-diaktifkan
- alb-http-to-https-pengalihan-periksa
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-penghapusan-diaktifkan
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-diaktifkan
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-tidak-kosong
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-environment-description
- appconfig-environment-tagged

- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-penyimpanan
- appconfig-hosted-configuration-version-deskripsi
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-penerusan
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-default-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-akses
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check

- appsync-cache-ct-encryption-saat istirahat
- appsync-cache-ct-encryption-dalam transit
- appsync-cache-encryption-at-istirahat
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-istirahat
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapusan-dinonaktifkan

- backup-recovery-point-minimum-pemeriksaan retensi
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-diaktifkan
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-periksa
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-dikonfigurasi
- cloudfront-no-deprecated-ssl-protokol
- cloudfront-origin-access-identity-diaktifkan
- cloudfront-origin-failover-enabled
- cloudfront-s3- origin-access-control-enabled
- cloudfront-s3- origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-dienkripsi
- cloudfront-viewer-policy-https

- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-periksa
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- codedeploy-auto-rollback-monitor-diaktifkan
- codedeploy-deployment-group-auto-rollback-diaktifkan
- codedeploy-deployment-group-outdated-instances-pembaruan
- codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan
- codeguruprofiler-profiling-group-tagged

- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-akses-cek
- cognito-user-pool-advanced-keamanan diaktifkan
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-pembuatan profil
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-Terlampir
- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-tingkatkan periksa
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-diaktifkan
- dms-neptune-iam-authorization-diaktifkan
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged

- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-diaktifkan
- docdb-cluster-backup-retention-periksa
- docdb-cluster-deletion-protection-diaktifkan
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-dilarang
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- diaktifkan client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -semua client-vpn-not-authorize

- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- diaktifkan enis-source-destination-check
- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- dibuat last-backup-recovery-point
- ec2- 2-periksa launch-template-imdsv
- ec2- launch-template-public-ip -dinonaktifkan
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -periksa managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- network-insights-access-scope -analisis ditandai
- ec2- -ditandai network-insights-access-scope
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2- resources-in-logically-air -gapped-lemari besi

- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2- security-group-attached-to -eni-periodik
- ec2- - spot-fleet-request-ct encryption-at-rest
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan
- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi
- ecs-task-definition-memory-batas-keras

- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-pengguna
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan
- terlampir eip
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versi
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan
- elasticache-repl-grp-encrypted-saat istirahat

- elasticache-repl-grp-encrypted-dalam transit
- elasticache-repl-grp-redis-auth-diaktifkan
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-logs-to-jam tangan awan
- elastic-beanstalk-managed-updates-diaktifkan
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -periksa predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-istirahat
- emr-security-configuration-encryption-transit

- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-konfigurasi-ada
- fis-experiment-template-tagged
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-dibuat
- fsx-lustre-copy-tagsuntuk-backup
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-audit-log-dikonfigurasi
- fsx-windows-deployment-type-periksa
- glb-listener-tagged
- global-endpoint-event-replication-diaktifkan
- glue-job-logging-enabled

- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-tindakan
- iam-external-access-analyzer-diaktifkan
- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa
- iam-oidc-provider-tagged
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa
- iam-root-access-key-periksa
- iam-saml-provider-tagged
- iam-server-certificate-expiration-periksa
- iam-server-certificate-tagged

- iam-user-group-membership-periksa
- iam-user-mfa-enabled
- iam-user-no-policies-periksa
- iam-user-unused-credentials-periksa
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-diaktifkan
- inspector-lambda-standard-scan-diaktifkan
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-diaktifkan
- ivs-channel-playback-authorization-diaktifkan

- ivs-channel-tagged
- ivs-playback-key-pair-ditandai
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-penemuan-cek
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-log
- mfa-enabled-for-iam-akses konsol
- mq-active-broker-ldap-otentikasi
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade diaktifkan
- mq-auto-minor-version-upgrade diaktifkan
- mq-broker-general-logging-diaktifkan
- mq-cloudwatch-audit-logging-diaktifkan

- mq-cloudwatch-audit-log-diaktifkan
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-dinonaktifkan
- msk-connect-connector-logging-diaktifkan
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-periksa
- neptune-cluster-cloudwatch-log-ekspor diaktifkan
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-diaktifkan
- neptune-cluster-encrypted
- neptune-cluster-iam-database-otentikasi
- neptune-cluster-multi-az-diaktifkan
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-dilarang
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-cross-zone-load-menyeimbangkan diaktifkan
- nlb-internal-scheme-check

- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-toleransi
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-pemeriksaan enkripsi-
- opensearch-primary-node-fault-toleransi
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-aurora-postgresql-logske cloudwatch
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-db-security-group-tidak diizinkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa

- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-diaktifkan
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan

- redshift-require-tls-ssl
- redshift-serverless-default-admin-periksa
- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi
- redshift-serverless-publish-logske cloudwatch
- redshift-serverless-workgroup-encrypted-dalam transit
- redshift-serverless-workgroup-no-akses publik
- redshift-serverless-workgroup-routes-dalam-vpc
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- rute53- query-logging-enabled
- s3 -aturan-periksa express-dir-bucket-lifecycle
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited

- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -gapped-lemari besi
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-ditandai
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-instance-root-akses-cek
- sagemaker-notebook-no-direct-akses internet

- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-notifikasi-diaktifkan
- sns-topic-no-public-akses
- sqs-queue-no-public-akses
- ssm-automation-block-public-berbagi
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged

- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-dibuat
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-rencana cadangan
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-peering-dns-resolution-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-kosong
- waf-global-rule-not-kosong
- waf-global-webacl-not-kosong
- waf-regional-rulegroup-not-kosong
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong
- workspaces-root-volume-encryption-diaktifkan

- workspaces-user-volume-encryption-diaktifkan

Daftar Aturan AWS Config Terkelola berdasarkan Jenis Pemicu

AWS Config saat ini mendukung aturan terkelola berikut. Sebelum menggunakan aturan ini, lihatPertimbangan.

Perubahan Konfigurasi

Aturan yang dipicu perubahan adalah aturan yang AWS Config mengevaluasi sebagai respons terhadap perubahan konfigurasi.

Perubahan Konfigurasi

- acmpca-certificate-authority-tagged
- acm-certificate-rsa-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-diaktifkan
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-penghapusan-diaktifkan
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-diaktifkan
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan

- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-tidak-kosong
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-penyimpanan
- appconfig-hosted-configuration-version-deskripsi
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-penerusan
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-default-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged

- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-akses
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-authorization-check
- appsync-cache-ct-encryption-saat istirahat
- appsync-cache-ct-encryption-dalam transit
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-istirahat
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled
- aurora-mysql-backtracking-enabled
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types

- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapusan-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-diaktifkan
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-dikonfigurasi
- cloudfront-no-deprecated-ssl-protokol
- cloudfront-origin-access-identity-diaktifkan
- cloudfront-origin-failover-enabled
- cloudfront-s3- origin-access-control-enabled
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-ssl-policy-check

- cloudfront-traffic-to-origin-dienkripsi
- cloudfront-viewer-policy-https
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-settings-check
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-periksa
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- codedeploy-auto-rollback-monitor-diaktifkan
- codedeploy-deployment-group-auto-rollback-diaktifkan
- codedeploy-deployment-group-outdated-instances-pembaruan
- codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-akses-cek
- cognito-user-pool-advanced-keamanan diaktifkan
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-pembuatan profil
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached

- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-tingkatkan periksa
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-diaktifkan
- dms-neptune-iam-authorization-diaktifkan
- dms-redis-tls-enabled
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-diaktifkan
- docdb-cluster-backup-retention-periksa
- docdb-cluster-deletion-protection-diaktifkan
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-dilarang
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- ebs-optimized-instance
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- diaktifkan client-vpn-connection-log

- ec2- client-vpn-endpoint-tagged
- ec2- dhcp-options-tagged
- ec2- diaktifkan enis-source-destination-check
- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- 2-periksa launch-template-imdsv
- ec2- launch-template-public-ip -dinonaktifkan
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -periksa managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- network-insights-access-scope -analisis ditandai
- ec2- -ditandai network-insights-access-scope
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2- -eni security-group-attached-to
- ec2- - spot-fleet-request-ct encryption-at-rest
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description

- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan
- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi
- ecs-task-definition-memory-batas-keras
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-pengguna
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-filesystem-ct-encrypted

- terlampir eip
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versi
- eks-cluster-supported-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-logs-to-jam tangan awan
- elastic-beanstalk-managed-updates-diaktifkan
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -periksa predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-security-configuration-encryption-istirahat
- emr-security-configuration-encryption-transit
- volume terenkripsi
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description

- evidently-segment-tagged
- fis-experiment-template-log-konfigurasi-ada
- fis-experiment-template-tagged
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- glb-listener-tagged
- global-endpoint-event-replication-diaktifkan
- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- iam-customer-policy-blocked-kms-tindakan
- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa
- iam-oidc-provider-tagged
- iam-policy-blacklisted-check
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa
- iam-saml-provider-tagged
- iam-server-certificate-tagged
- iam-user-group-membership-periksa
- iam-user-no-policies-periksa
- instances-in-vpc

- internet-gateway-authorized-vpc-hanya
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-diaktifkan
- ivs-channel-playback-authorization-diaktifkan
- ivs-channel-tagged
- ivs-playback-key-pair-ditandai
- ivs-recording-configuration-tagged
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check

- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- mq-active-broker-ldap-otentikasi
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-upgrade diaktifkan
- mq-broker-general-logging-diaktifkan
- mq-cloudwatch-audit-log-diaktifkan
- mq-rabbit-deployment-mode
- msk-cluster-public-access-dinonaktifkan
- msk-connect-connector-logging-diaktifkan
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- msk-unrestricted-access-check
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-periksa
- neptune-cluster-cloudwatch-log-ekspor diaktifkan
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-diaktifkan
- neptune-cluster-encrypted
- neptune-cluster-iam-database-otentikasi
- neptune-cluster-multi-az-diaktifkan
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-dilarang
- netfw-deletion-protection-enabled

- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-cross-zone-load-menyeimbangkan diaktifkan
- nlb-internal-scheme-check
- nlb-listener-tagged
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-toleransi
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-pemeriksaan enkripsi-
- opensearch-primary-node-fault-toleransi
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-aurora-postgresql-logske cloudwatch
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan

- rds-db-security-group-tidak diizinkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-logging-enabled
- rds-multi-az-support
- rds-postgresql-logs-to-jam tangan awan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-diaktifkan
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- tag yang dibutuhkan
- rute53- query-logging-enabled
- s3 -aturan-periksa express-dir-bucket-lifecycle

- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-ember dengan tag
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- lifecycle-policy-check
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-ditandai
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled

- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-akses-cek
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-using-cmk
- service-catalog-shared-within-organisasi
- sns-encrypted-kms
- sns-topic-message-delivery-notifikasi-diaktifkan
- sns-topic-no-public-akses
- sqs-queue-no-public-akses
- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-tertutup
- vpc-network-acl-unused-periksa
- vpc-peering-dns-resolution-periksa
- vpc-vpn-2-terowongan
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty

- waf-global-rulegroup-not-kosong
- waf-global-rule-not-kosong
- waf-global-webacl-not-kosong
- waf-regional-rulegroup-not-kosong
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong
- workspaces-root-volume-encryption-diaktifkan
- workspaces-user-volume-encryption-diaktifkan

Berkala

Aturan periodik adalah aturan yang AWS Config mengevaluasi secara periodis pada frekuensi yang Anda tentukan; misalnya, setiap 24 jam.

Berkala

- access-keys-rotated
- account-part-of-organizations
- acm-pca-root-ca-dinonaktifkan
- alb-http-to-https-pengalihan-periksa
- api-gwv2- authorization-type-configured
- appsync-associated-with-waf
- appsync-cache-encryption-at-istirahat
- aurora-last-backup-recovery-point-dibuat
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- cloudfront-s3- origin-non-existent-bucket
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check

- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- custom-schema-registry-policy-Terlampir
- cw-loggroup-retention-period-periksa
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- dms-replication-not-public
- docdb-cluster-encrypted-in-transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa

- ec2- -semua client-vpn-not-authorize
- ec2- ebs-encryption-by-default
- ec2- -dibuat last-backup-recovery-point
- ec2- meets-restore-time-target
- ec2- resources-in-logically-air -gapped-lemari besi
- ec2- -rencana resources-protected-by-backup
- ec2- security-group-attached-to -eni-periodik
- ec2-stopped-instance
- ecr-private-image-scanning-diaktifkan
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan
- eks-cluster-logging-enabled
- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan
- elasticache-repl-grp-encrypted-saat istirahat
- elasticache-repl-grp-encrypted-dalam transit
- elasticache-repl-grp-redis-auth-diaktifkan
- elasticache-subnet-group-check

- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elbv2- acm-certificate-required
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- event-data-store-cmk-enkripsi diaktifkan
- fsx-last-backup-recovery-point-dibuat
- fsx-lustre-copy-tagsuntuk-backup
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-audit-log-dikonfigurasi
- fsx-windows-deployment-type-periksa
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-diaktifkan

- iam-password-policy
- iam-policy-in-use
- iam-root-access-key-periksa
- iam-server-certificate-expiration-periksa
- iam-user-mfa-enabled
- iam-user-unused-credentials-periksa
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-diaktifkan
- inspector-lambda-standard-scan-diaktifkan
- kinesis-firehose-delivery-stream-dienkripsi
- kms-cmk-not-scheduled-untuk-penghapusan
- macie-auto-sensitive-data-penemuan-cek
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-log
- mfa-enabled-for-iam-akses konsol
- mq-automatic-minor-version-upgrade diaktifkan
- mq-cloudwatch-audit-logging-diaktifkan
- mq-no-public-access
- multi-region-cloud-trail-diaktifkan
- netfw-logging-enabled
- nlb-logging-enabled
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-mariadb-instance-encrypted-dalam transit
- rds-meets-restore-time-target
- rds-mysql-instance-encrypted-dalam transit
- rds-postgres-instance-encrypted-dalam transit

- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-sqlserver-encrypted-in-transit
- redshift-serverless-default-admin-periksa
- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi
- redshift-serverless-publish-logske cloudwatch
- redshift-serverless-workgroup-encrypted-dalam transit
- redshift-serverless-workgroup-no-akses publik
- redshift-serverless-workgroup-routes-dalam-vpc
- redshift-unrestricted-port-access
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- s3- account-level-public-access -blok-periodik
- s3- -dibuat last-backup-recovery-point
- s3- meets-restore-time-target
- s3- resources-in-logically-air -gapped-lemari besi
- s3- -rencana resources-protected-by-backup
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-no-direct-akses internet
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- Securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled

- shield-advanced-enabled-autorenew
- shield-drt-access
- ssm-automation-block-public-berbagi
- ssm-automation-logging-enabled
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-dibuat
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-rencana cadangan
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-sg-port-restriction-periksa
- wafv2-logging-diaktifkan
- waf-classic-logging-enabled

Hibrida

Aturan hibrida adalah aturan yang AWS Config mengevaluasi baik dalam menanggapi perubahan konfigurasi dan periodis.

Hibrida

- acm-certificate-expiration-check
- cloudformation-stack-drift-detection-periksa
- ec2- -ami instance-launched-with-allowed
- incoming-ssh-disabled
- no-unrestricted-route-to-igw
- restricted-incoming-traffic

- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- vpc-sg-open-only-to-authorized-ports

Daftar Aturan AWS Config Terkelola berdasarkan Ketersediaan Wilayah

AWS Config saat ini mendukung aturan terkelola berikut. Sebelum menggunakan aturan ini, lihatPertimbangan.

Wilayah AS Timur (Ohio)

AS Timur (Ohio)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pemeriksaan-pengalihan
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-penghapusan-diaktifkan
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-diaktifkan
- amplify-branch-tagged

- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-tidak-kosong
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-penyimpanan
- appconfig-hosted-configuration-version-deskripsi
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-penerusan
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-default-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists

- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-akses
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-istirahat
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-istirahat
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-capacity-rebalancing

- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapusan-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-diaktifkan
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-periksa
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited

- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-periksa
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- codedeploy-auto-rollback-monitor-diaktifkan
- codedeploy-deployment-group-auto-rollback-diaktifkan
- codedeploy-deployment-group-outdated-instances-pembaruan
- codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-akses-cek

- cognito-user-pool-advanced-keamanan diaktifkan
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-Terlampir
- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-tingkatkan periksa
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-diaktifkan
- dms-neptune-iam-authorization-diaktifkan
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-diaktifkan
- docdb-cluster-backup-retention-periksa
- docdb-cluster-deletion-protection-diaktifkan
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-dilarang

- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- diaktifkan client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -semua client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- diaktifkan enis-source-destination-check
- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed

- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -dibuat last-backup-recovery-point
- ec2- 2-periksa launch-template-imdsv
- ec2- launch-template-public-ip -dinonaktifkan
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -periksa managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- network-insights-access-scope -analisis ditandai
- ec2- -ditandai network-insights-access-scope
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- resources-in-logically-air -gapped-lemari besi
- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2- security-group-attached-to -eni-periodik
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description

- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan
- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi
- ecs-task-definition-memory-batas-keras
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-pengguna
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted

- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan
- terlampir eip
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versi
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan
- elasticache-repl-grp-encrypted-saat istirahat
- elasticache-repl-grp-encrypted-dalam transit
- elasticache-repl-grp-redis-auth-diaktifkan
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only

- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-logs-to-jam tangan awan
- elastic-beanstalk-managed-updates-diaktifkan
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -periksa predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-istirahat
- emr-security-configuration-encryption-transit
- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-konfigurasi-ada

- fis-experiment-template-tagged
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-dibuat
- fsx-lustre-copy-tagsuntuk-backup
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-audit-log-dikonfigurasi
- fsx-windows-deployment-type-periksa
- glb-listener-tagged
- global-endpoint-event-replication-diaktifkan
- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled

- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-tindakan
- iam-external-access-analyzer-diaktifkan
- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa
- iam-root-access-key-periksa
- iam-user-group-membership-periksa
- iam-user-mfa-enabled
- iam-user-no-policies-periksa
- iam-user-unused-credentials-periksa
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-diaktifkan
- inspector-lambda-standard-scan-diaktifkan
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged

- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iot-authorizer-token-signing-diaktifkan
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-penemuan-cek
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-log
- mfa-enabled-for-iam-akses konsol
- mq-active-broker-ldap-otentikasi
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs

- mq-automatic-minor-version-upgrade diaktifkan
- mq-auto-minor-version-upgrade diaktifkan
- mq-broker-general-logging-diaktifkan
- mq-cloudwatch-audit-logging-diaktifkan
- mq-cloudwatch-audit-log-diaktifkan
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-dinonaktifkan
- msk-connect-connector-logging-diaktifkan
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-periksa
- neptune-cluster-cloudwatch-log-ekspor diaktifkan
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-diaktifkan
- neptune-cluster-encrypted
- neptune-cluster-iam-database-otentikasi
- neptune-cluster-multi-az-diaktifkan
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-dilarang
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait

- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-cross-zone-load-menyeimbangkan diaktifkan
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-toleransi
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-pemeriksaan enkripsi-
- opensearch-primary-node-fault-toleransi
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-aurora-postgresql-logske cloudwatch
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa

- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-diaktifkan
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az

- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-serverless-default-admin-periksa
- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi
- redshift-serverless-publish-logske cloudwatch
- redshift-serverless-workgroup-encrypted-dalam transit
- redshift-serverless-workgroup-no-akses publik
- redshift-serverless-workgroup-routes-dalam-vpc
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- s3 -aturan-periksa express-dir-bucket-lifecycle
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check

- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -gapped-lemari besi
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-ditandai
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi

- sagemaker-notebook-instance-root-akses-cek
- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub diaktifkan
- security-account-information-provided
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notifikasi-diaktifkan
- sns-topic-no-public-akses
- sqs-queue-no-public-akses
- ssm-automation-block-public-berbagi
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled

- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-dibuat
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-rencana cadangan
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-peering-dns-resolution-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-kosong
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong

Wilayah AS Timur (Virginia Utara)

AS Timur (Virginia Utara)

- access-keys-rotated
- account-part-of-organizations

- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pemeriksaan-pengalihan
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-penghapusan-diaktifkan
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-diaktifkan
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-tidak-kosong
- appconfig-deployment-strategy-description

- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-penyimpanan
- appconfig-hosted-configuration-version-deskripsi
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-penerusan
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-default-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-akses
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc

- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-saat istirahat
- appsync-cache-ct-encryption-dalam transit
- appsync-cache-encryption-at-istirahat
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-istirahat
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted

- backup-recovery-point-manual-penghapusan-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-diaktifkan
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-periksa
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-dikonfigurasi
- cloudfront-no-deprecated-ssl-protokol
- cloudfront-origin-access-identity-diaktifkan
- cloudfront-origin-failover-enabled
- cloudfront-s3- origin-access-control-enabled
- cloudfront-s3- origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-dienkripsi

- cloudfront-viewer-policy-https
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-periksa
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- codedeploy-auto-rollback-monitor-diaktifkan
- codedeploy-deployment-group-auto-rollback-diaktifkan
- codedeploy-deployment-group-outdated-instances-pembaruan
- codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan

- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-akses-cek
- cognito-user-pool-advanced-keamanan diaktifkan
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-pembuatan profil
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-Terlampir
- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-tingkatkan periksa
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-diaktifkan
- dms-neptune-iam-authorization-diaktifkan
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging

- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-diaktifkan
- docdb-cluster-backup-retention-periksa
- docdb-cluster-deletion-protection-diaktifkan
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-dilarang
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- diaktifkan client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged

- ec2- -semua client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- diaktifkan enis-source-destination-check
- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -dibuat last-backup-recovery-point
- ec2- 2-periksa launch-template-imdsv
- ec2- launch-template-public-ip -dinonaktifkan
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -periksa managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- network-insights-access-scope -analisis ditandai
- ec2- -ditandai network-insights-access-scope
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged

- ec2- resources-in-logically-air -gapped-lemari besi
- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2- security-group-attached-to -eni-periodik
- ec2- - spot-fleet-request-ct encryption-at-rest
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan
- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi

- ecs-task-definition-memory-batas-keras
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-pengguna
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan
- terlampir eip
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versi
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan

- elasticache-repl-grp-encrypted-saat istirahat
- elasticache-repl-grp-encrypted-dalam transit
- elasticache-repl-grp-redis-auth-diaktifkan
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-logs-to-jam tangan awan
- elastic-beanstalk-managed-updates-diaktifkan
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -periksa predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-istirahat

- emr-security-configuration-encryption-transit
- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-konfigurasi-ada
- fis-experiment-template-tagged
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-dibuat
- fsx-lustre-copy-tagsuntuk-backup
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-audit-log-dikonfigurasi
- fsx-windows-deployment-type-periksa
- glb-listener-tagged
- global-endpoint-event-replication-diaktifkan

- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-tindakan
- iam-external-access-analyzer-diaktifkan
- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa
- iam-oidc-provider-tagged
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa
- iam-root-access-key-periksa
- iam-saml-provider-tagged
- iam-server-certificate-expiration-periksa

- iam-server-certificate-tagged
- iam-user-group-membership-periksa
- iam-user-mfa-enabled
- iam-user-no-policies-periksa
- iam-user-unused-credentials-periksa
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-diaktifkan
- inspector-lambda-standard-scan-diaktifkan
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-diaktifkan

- ivs-channel-playback-authorization-diaktifkan
- ivs-channel-tagged
- ivs-playback-key-pair-ditandai
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-penemuan-cek
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-log
- mfa-enabled-for-iam-akses konsol
- mq-active-broker-ldap-otentikasi
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade diaktifkan
- mq-auto-minor-version-upgrade diaktifkan
- mq-broker-general-logging-diaktifkan

- mq-cloudwatch-audit-logging-diaktifkan
- mq-cloudwatch-audit-log-diaktifkan
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-dinonaktifkan
- msk-connect-connector-logging-diaktifkan
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-periksa
- neptune-cluster-cloudwatch-log-ekspor diaktifkan
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-diaktifkan
- neptune-cluster-encrypted
- neptune-cluster-iam-database-otentikasi
- neptune-cluster-multi-az-diaktifkan
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-dilarang
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-cross-zone-load-menyeimbangkan diaktifkan

- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-toleransi
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-pemeriksaan enkripsi-
- opensearch-primary-node-fault-toleransi
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-aurora-postgresql-logske cloudwatch
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-db-security-group-tidak diizinkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan

- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-diaktifkan
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-periksa

- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-serverless-default-admin-periksa
- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi
- redshift-serverless-publish-logske cloudwatch
- redshift-serverless-workgroup-encrypted-dalam transit
- redshift-serverless-workgroup-no-akses publik
- redshift-serverless-workgroup-routes-dalam-vpc
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- rute53- query-logging-enabled
- s3 -aturan-periksa express-dir-bucket-lifecycle
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif

- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -gapped-lemari besi
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-ditandai
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-instance-root-akses-cek

- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-notifikasi-diaktifkan
- sns-topic-no-public-akses
- sqs-queue-no-public-akses
- ssm-automation-block-public-berbagi
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description

- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-dibuat
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-rencana cadangan
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-peering-dns-resolution-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-kosong
- waf-global-rule-not-kosong
- waf-global-webacl-not-kosong
- waf-regional-rulegroup-not-kosong
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong

- workspaces-root-volume-encryption-diaktifkan
- workspaces-user-volume-encryption-diaktifkan

Wilayah AS Barat (California Utara)

AS Barat (California Utara)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pemeriksaan-pengalihan
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-penghapusan-diaktifkan
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-diaktifkan
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa

- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-tidak-kosong
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-penyimpanan
- appconfig-hosted-configuration-version-deskripsi
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-penerusan
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-default-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag

- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-istirahat
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-istirahat
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapusan-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi

- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-diaktifkan
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-periksa
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan

- cmk-backing-key-rotation-diaktifkan
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-periksa
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- codedeploy-auto-rollback-monitor-diaktifkan
- codedeploy-deployment-group-auto-rollback-diaktifkan
- codedeploy-deployment-group-outdated-instances-pembaruan
- codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-akses-cek
- cognito-user-pool-advanced-keamanan diaktifkan
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-Terlampir
- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type

- dms-auto-minor-version-tingkatkan periksa
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-diaktifkan
- dms-neptune-iam-authorization-diaktifkan
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- diaktifkan client-vpn-connection-log

- ec2- client-vpn-endpoint-tagged
- ec2- -semua client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- diaktifkan enis-source-destination-check
- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -dibuat last-backup-recovery-point
- ec2- 2-periksa launch-template-imdsv
- ec2- launch-template-public-ip -dinonaktifkan
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -periksa managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- network-insights-access-scope -analisis ditandai
- ec2- -ditandai network-insights-access-scope
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check

- ec2- prefix-list-tagged
- ec2- resources-in-logically-air -gapped-lemari besi
- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2- security-group-attached-to -eni-periodik
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan
- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi

- ecs-task-definition-memory-batas-keras
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-pengguna
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan
- terlampir eip
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versi
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan

- elasticache-repl-grp-encrypted-saat istirahat
- elasticache-repl-grp-encrypted-dalam transit
- elasticache-repl-grp-redis-auth-diaktifkan
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-logs-to-jam tangan awan
- elastic-beanstalk-managed-updates-diaktifkan
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -periksa predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-istirahat

- emr-security-configuration-encryption-transit
- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan
- fis-experiment-template-log-konfigurasi-ada
- fis-experiment-template-tagged
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- fsx-last-backup-recovery-point-dibuat
- fsx-lustre-copy-tagsuntuk cadangan
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-audit-log-dikonfigurasi
- fsx-windows-deployment-type-periksa
- glb-listener-tagged
- global-endpoint-event-replication-diaktifkan
- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled

- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-tindakan
- iam-external-access-analyzer-diaktifkan
- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa
- iam-root-access-key-periksa
- iam-user-group-membership-periksa
- iam-user-mfa-enabled
- iam-user-no-policies-periksa
- iam-user-unused-credentials-periksa
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-diaktifkan
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- iot-authorizer-token-signing-diaktifkan
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa

- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- macie-auto-sensitive-data-penemuan-cek
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-log
- mfa-enabled-for-iam-akses konsol
- mq-active-broker-ldap-otentikasi
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade diaktifkan
- mq-auto-minor-version-upgrade diaktifkan
- mq-broker-general-logging-diaktifkan
- mq-cloudwatch-audit-logging-diaktifkan
- mq-cloudwatch-audit-log-diaktifkan
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-dinonaktifkan
- msk-connect-connector-logging-diaktifkan
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- msk-unrestricted-access-check

- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-periksa
- neptune-cluster-cloudwatch-log-ekspor diaktifkan
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-diaktifkan
- neptune-cluster-encrypted
- neptune-cluster-iam-database-otentikasi
- neptune-cluster-multi-az-diaktifkan
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-dilarang
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-cross-zone-load-menyeimbangkan diaktifkan
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-toleransi
- opensearch-encrypted-at-rest
- opensearch-https-required

- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-pemeriksaan enkripsi-
- opensearch-primary-node-fault-toleransi
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-aurora-postgresql-logske cloudwatch
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-db-security-group-tidak diizinkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan

- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-serverless-default-admin-periksa
- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi
- redshift-serverless-publish-logske cloudwatch
- redshift-serverless-workgroup-encrypted-dalam transit
- redshift-serverless-workgroup-no-akses publik
- redshift-serverless-workgroup-routes-dalam-vpc
- redshift-unrestricted-port-access
- tag yang dibutuhkan

- restricted-incoming-traffic
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -gapped-lemari besi

- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-ditandai
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-instance-root-akses-cek
- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub diaktifkan
- security-account-information-provided
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notifikasi-diaktifkan
- sns-topic-no-public-akses

- sqs-queue-no-public-akses
- ssm-automation-block-public-berbagi
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-dibuat
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-rencana cadangan
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-peering-dns-resolution-periksa
- vpc-sg-open-only-to-authorized-ports

- vpc-sg-port-restriction-periksa
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-kosong
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong

Wilayah AS Barat (Oregon)

AS Barat (Oregon)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pemeriksaan-pengalihan
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-penghapusan-diaktifkan
- amplify-app-description
- amplify-app-tagged

- amplify-branch-performance-mode-diaktifkan
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-tidak-kosong
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-penyimpanan
- appconfig-hosted-configuration-version-deskripsi
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-penerusan
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-default-tls

- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-akses
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-istirahat
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-istirahat
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled

- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapusan-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-diaktifkan
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-periksa
- cloudformation-stack-notification-check

- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-periksa
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- codedeploy-auto-rollback-monitor-diaktifkan
- codedeploy-deployment-group-auto-rollback-diaktifkan
- codedeploy-deployment-group-outdated-instances-pembaruan
- codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan
- codeguruprofiler-profiling-group-tagged

- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-akses-cek
- cognito-user-pool-advanced-keamanan diaktifkan
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-pembuatan profil
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-Terlampir
- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-tingkatkan periksa
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-diaktifkan
- dms-neptune-iam-authorization-diaktifkan
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged

- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-diaktifkan
- docdb-cluster-backup-retention-periksa
- docdb-cluster-deletion-protection-diaktifkan
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-dilarang
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- diaktifkan client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -semua client-vpn-not-authorize

- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- diaktifkan enis-source-destination-check
- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -dibuat last-backup-recovery-point
- ec2- 2-periksa launch-template-imdsv
- ec2- launch-template-public-ip -dinonaktifkan
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -periksa managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- network-insights-access-scope -analisis ditandai
- ec2- -ditandai network-insights-access-scope
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2- resources-in-logically-air -gapped-lemari besi

- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2- security-group-attached-to -eni-periodik
- ec2- - spot-fleet-request-ct encryption-at-rest
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan
- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi
- ecs-task-definition-memory-batas-keras

- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-pengguna
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan
- terlampir eip
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versi
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan
- elasticache-repl-grp-encrypted-saat istirahat

- elasticache-repl-grp-encrypted-dalam transit
- elasticache-repl-grp-redis-auth-diaktifkan
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-logs-to-jam tangan awan
- elastic-beanstalk-managed-updates-diaktifkan
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -periksa predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-istirahat
- emr-security-configuration-encryption-transit

- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-konfigurasi-ada
- fis-experiment-template-tagged
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-dibuat
- fsx-lustre-copy-tagsuntuk cadangan
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-audit-log-dikonfigurasi
- fsx-windows-deployment-type-periksa
- glb-listener-tagged
- global-endpoint-event-replication-diaktifkan
- glue-job-logging-enabled

- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-tindakan
- iam-external-access-analyzer-diaktifkan
- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa
- iam-root-access-key-periksa
- iam-user-group-membership-periksa
- iam-user-mfa-enabled
- iam-user-no-policies-periksa
- iam-user-unused-credentials-periksa

- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-diaktifkan
- inspector-lambda-standard-scan-diaktifkan
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-diaktifkan
- ivs-channel-playback-authorization-diaktifkan
- ivs-channel-tagged
- ivs-playback-key-pair-ditandai
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-dienkripsi

- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-penemuan-cek
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-log
- mfa-enabled-for-iam-akses konsol
- mq-active-broker-ldap-otentikasi
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade diaktifkan
- mq-auto-minor-version-upgrade diaktifkan
- mq-broker-general-logging-diaktifkan
- mq-cloudwatch-audit-logging-diaktifkan
- mq-cloudwatch-audit-log-diaktifkan
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-dinonaktifkan

- msk-connect-connector-logging-diaktifkan
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-periksa
- neptune-cluster-cloudwatch-log-ekspor diaktifkan
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-diaktifkan
- neptune-cluster-encrypted
- neptune-cluster-iam-database-otentikasi
- neptune-cluster-multi-az-diaktifkan
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-dilarang
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-cross-zone-load-menyeimbangkan diaktifkan
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled

- opensearch-audit-logging-enabled
- opensearch-data-node-fault-toleransi
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-pemeriksaan enkripsi-
- opensearch-primary-node-fault-toleransi
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-aurora-postgresql-logske cloudwatch
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-db-security-group-tidak diizinkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled

- rds-mariadb-instance-encrypted-dalam transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-diaktifkan
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-serverless-default-admin-periksa
- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi

- redshift-serverless-publish-logske cloudwatch
- redshift-serverless-workgroup-encrypted-dalam transit
- redshift-serverless-workgroup-no-akses publik
- redshift-serverless-workgroup-routes-dalam-vpc
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- s3 -aturan-periksa express-dir-bucket-lifecycle
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-bucket-tagged

- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -gapped-lemari besi
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-ditandai
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-instance-root-akses-cek
- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk

- Securityhub diaktifkan
- security-account-information-provided
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notifikasi-diaktifkan
- sns-topic-no-public-akses
- sqs-queue-no-public-akses
- ssm-automation-block-public-berbagi
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-dibuat

- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-rencana cadangan
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-peering-dns-resolution-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-kosong
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong
- workspaces-root-volume-encryption-diaktifkan
- workspaces-user-volume-encryption-diaktifkan

Wilayah Afrika (Cape Town)

Afrika (Cape Town)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan

- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pemeriksaan-pengalihan
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-tidak-kosong
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-penyimpanan
- appconfig-hosted-configuration-version-deskripsi
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged

- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-penerusan
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-default-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-istirahat
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-capacity-rebalancing

- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapusan-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-diaktifkan
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-periksa
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan

- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-periksa
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- codedeploy-auto-rollback-monitor-diaktifkan
- codedeploy-deployment-group-auto-rollback-diaktifkan
- codedeploy-deployment-group-outdated-instances-pembaruan
- codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan
- cognito-identity-pool-unauth-akses-cek
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-pembuatan profil
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached

- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-tingkatkan periksa
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-diaktifkan
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target
- ebs-optimized-instance

- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- diaktifkan client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -semua client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- diaktifkan enis-source-destination-check
- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -dibuat last-backup-recovery-point
- ec2- 2-periksa launch-template-imdsv
- ec2- launch-template-public-ip -dinonaktifkan
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- network-insights-access-scope -analisis ditandai

- ec2- -ditandai network-insights-access-scope
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- resources-in-logically-air -gapped-lemari besi
- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2- security-group-attached-to -eni-periodik
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan
- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi
- ecs-task-definition-memory-batas-keras
- ecs-task-definition-network-mode-not-host

- ecs-task-definition-nonroot-pengguna
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan
- terlampir eip
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versi
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan
- elasticache-repl-grp-encrypted-saat istirahat
- elasticache-repl-grp-encrypted-dalam transit

- elasticache-repl-grp-redis-auth-diaktifkan
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-logs-to-jam tangan awan
- elastic-beanstalk-managed-updates-diaktifkan
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -periksa predefined-security-policy-ssl
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-istirahat
- emr-security-configuration-encryption-transit
- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan

- fis-experiment-template-log-konfigurasi-ada
- fis-experiment-template-tagged
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- fsx-last-backup-recovery-point-dibuat
- fsx-lustre-copy-tagsuntuk cadangan
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-audit-log-dikonfigurasi
- fsx-windows-deployment-type-periksa
- glb-listener-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled

- iam-customer-policy-blocked-kms-tindakan
- iam-external-access-analyzer-diaktifkan
- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa
- iam-root-access-key-periksa
- iam-user-group-membership-periksa
- iam-user-mfa-enabled
- iam-user-no-policies-periksa
- iam-user-unused-credentials-periksa
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-diaktifkan
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check

- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- macie-auto-sensitive-data-penemuan-cek
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-log
- mfa-enabled-for-iam-akses konsol
- mq-active-broker-ldap-otentikasi
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-upgrade diaktifkan
- mq-broker-general-logging-diaktifkan
- mq-cloudwatch-audit-log-diaktifkan
- mq-rabbit-deployment-mode
- msk-cluster-public-access-dinonaktifkan
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-periksa
- neptune-cluster-cloudwatch-log-ekspor diaktifkan
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-diaktifkan
- neptune-cluster-encrypted
- neptune-cluster-iam-database-otentikasi
- neptune-cluster-multi-az-diaktifkan

- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-dilarang
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-cross-zone-load-menyeimbangkan diaktifkan
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-toleransi
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-pemeriksaan enkripsi-
- opensearch-primary-node-fault-toleransi
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-aurora-postgresql-logske cloudwatch
- rds-automatic-minor-version-upgrade diaktifkan

- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled

- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-diaktifkan
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif

- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-ditandai
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-instance-root-akses-cek
- sagemaker-notebook-no-direct-akses internet

- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub diaktifkan
- security-account-information-provided
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notifikasi-diaktifkan
- sns-topic-no-public-akses
- sqs-queue-no-public-akses
- ssm-automation-block-public-berbagi
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp

- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-dibuat
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-rencana cadangan
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-peering-dns-resolution-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-kosong
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong
- workspaces-root-volume-encryption-diaktifkan
- workspaces-user-volume-encryption-diaktifkan

Wilayah Asia Pasifik (Hong Kong)

Asia Pasifik (Hong Kong)

- access-keys-rotated
- account-part-of-organizations

- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pemeriksaan-pengalihan
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-penghapusan-diaktifkan
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-diaktifkan
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-tidak-kosong
- appconfig-deployment-strategy-description

- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-penyimpanan
- appconfig-hosted-configuration-version-deskripsi
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-penerusan
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-default-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-istirahat
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-istirahat
- athena-workgroup-enforce-workgroup-konfigurasi

- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapusan-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-diaktifkan
- cassandra-keyspace-tagged

- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-periksa
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-periksa
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- codedeploy-auto-rollback-monitor-diaktifkan
- codedeploy-deployment-group-auto-rollback-diaktifkan

- codedeploy-deployment-group-outdated-instances-pembaruan
- codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan
- codepipeline-deployment-count-check
- cognito-identity-pool-unauth-akses-cek
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-Terlampir
- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-tingkatkan periksa
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-diaktifkan
- dms-neptune-iam-authorization-diaktifkan
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-pencatatan
- dms-replication-task-tagged
- dms-replication-task-targetdb-pencatatan
- docdb-cluster-audit-logging-diaktifkan
- docdb-cluster-backup-retention-periksa
- docdb-cluster-deletion-protection-diaktifkan
- docdb-cluster-encrypted

- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-dilarang
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- diaktifkan client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -semua client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- diaktifkan enis-source-destination-check
- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed

- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -dibuat last-backup-recovery-point
- ec2- 2-periksa launch-template-imdsv
- ec2- launch-template-public-ip -dinonaktifkan
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -periksa managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- network-insights-access-scope -analisis ditandai
- ec2- -ditandai network-insights-access-scope
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- resources-in-logically-air -gapped-lemari besi
- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2- security-group-attached-to -eni-periodik
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description

- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan
- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi
- ecs-task-definition-memory-batas-keras
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-pengguna
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted

- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan
- terlampir eip
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versi
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan
- elasticache-repl-grp-encrypted-saat istirahat
- elasticache-repl-grp-encrypted-dalam transit
- elasticache-repl-grp-redis-auth-diaktifkan
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only

- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-logs-to-jam tangan awan
- elastic-beanstalk-managed-updates-diaktifkan
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -periksa predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-istirahat
- emr-security-configuration-encryption-transit
- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan
- fis-experiment-template-log-konfigurasi-ada
- fis-experiment-template-tagged
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- fsx-last-backup-recovery-point-dibuat
- fsx-lustre-copy-tagsuntuk cadangan

- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-audit-log-dikonfigurasi
- fsx-windows-deployment-type-periksa
- glb-listener-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-tindakan
- iam-external-access-analyzer-diaktifkan
- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa
- iam-password-policy
- iam-policy-blacklisted-check

- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa
- iam-root-access-key-periksa
- iam-user-group-membership-periksa
- iam-user-mfa-enabled
- iam-user-no-policies-periksa
- iam-user-unused-credentials-periksa
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-diaktifkan
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- iot-authorizer-token-signing-diaktifkan
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- macie-auto-sensitive-data-penemuan-cek

- macie-status-check
- mariadb-publish-logs-to-cloudwatch-log
- mfa-enabled-for-iam-akses konsol
- mq-active-broker-ldap-otentikasi
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade diaktifkan
- mq-auto-minor-version-upgrade diaktifkan
- mq-broker-general-logging-diaktifkan
- mq-cloudwatch-audit-logging-diaktifkan
- mq-cloudwatch-audit-log-diaktifkan
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-dinonaktifkan
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-periksa
- neptune-cluster-cloudwatch-log-ekspor diaktifkan
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-diaktifkan
- neptune-cluster-encrypted
- neptune-cluster-iam-database-otentikasi
- neptune-cluster-multi-az-diaktifkan
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-dilarang
- netfw-deletion-protection-enabled

- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-cross-zone-load-menyeimbangkan diaktifkan
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-toleransi
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-pemeriksaan enkripsi-
- opensearch-primary-node-fault-toleransi
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-aurora-postgresql-logske cloudwatch
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan

- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled

- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-diaktifkan
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-serverless-default-admin-periksa
- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi
- redshift-serverless-publish-logske cloudwatch
- redshift-serverless-workgroup-no-akses publik
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled

- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-ember dengan tag
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-ditandai
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi

- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-instance-root-akses-cek
- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notifikasi-diaktifkan
- sns-topic-no-public-akses
- sqs-queue-no-public-akses
- ssm-automation-block-public-berbagi
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged

- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-dibuat
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-rencana cadangan
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-peering-dns-resolution-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-kosong
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong

Wilayah Asia Pasifik (Hyderabad)

Asia Pasifik (Hyderabad)

- account-part-of-organizations

- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan
- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pemeriksaan-pengalihan
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled

- aurora-last-backup-recovery-point-dibuat
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-pencatatan
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapusan-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited

- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public

- docdb-cluster-audit-logging-diaktifkan
- docdb-cluster-backup-retention-periksa
- docdb-cluster-deletion-protection-diaktifkan
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-dilarang
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed

- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -dibuat last-backup-recovery-point
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- prefix-list-tagged
- ec2- resources-in-logically-air -gapped-lemari besi
- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2-stopped-instance
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan
- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access

- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan
- terlampir eip
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan
- elasticache-repl-grp-encrypted-saat istirahat

- elasticache-repl-grp-encrypted-dalam transit
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-istirahat
- emr-security-configuration-encryption-transit
- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- fsx-last-backup-recovery-point-dibuat
- fsx-lustre-copy-tagsuntuk cadangan
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa

- fsx-resources-protected-by-rencana cadangan
- fsx-windows-audit-log-dikonfigurasi
- fsx-windows-deployment-type-periksa
- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-diaktifkan
- iam-password-policy
- iam-root-access-key-periksa
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- lambda-concurrency-check

- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- mariadb-publish-logs-to-cloudwatch-log
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-enhanced-monitoring-enabled

- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-periksa

- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-ember dengan tag
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point

- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub diaktifkan
- security-account-information-provided
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-akses
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-certificate-description
- transfer-certificate-tagged

- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong

Wilayah Asia Pasifik (Jakarta)

Asia Pasifik (Jakarta)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan

- alb-http-to-https-pemeriksaan-pengalihan
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-tidak-kosong
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-penyimpanan
- appconfig-hosted-configuration-version-deskripsi
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-penerusan
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-default-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists

- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-istirahat
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapusan-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi

- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-report-group-encrypted-saat istirahat
- cognito-identity-pool-unauth-akses-cek
- cognito-user-pool-tagged

- custom-eventbus-policy-attached
- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- diaktifkan enis-source-destination-check

- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -dibuat last-backup-recovery-point
- ec2- 2-periksa launch-template-imdsv
- ec2- launch-template-public-ip -dinonaktifkan
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- prefix-list-tagged
- ec2- resources-in-logically-air -gapped-lemari besi
- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2-stopped-instance
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan
- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled

- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan
- terlampir eip
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted

- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan
- elasticache-repl-grp-encrypted-saat istirahat
- elasticache-repl-grp-encrypted-dalam transit
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-logs-to-jam tangan awan
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-istirahat

- emr-security-configuration-encryption-transit
- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- fsx-last-backup-recovery-point-dibuat
- fsx-lustre-copy-tagsuntuk cadangan
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-audit-log-dikonfigurasi
- fsx-windows-deployment-type-periksa
- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-tindakan

- iam-external-access-analyzer-diaktifkan
- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa
- iam-root-access-key-periksa
- iam-user-group-membership-periksa
- iam-user-mfa-enabled
- iam-user-no-policies-periksa
- iam-user-unused-credentials-periksa
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-diaktifkan
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang

- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- mariadb-publish-logs-to-cloudwatch-log
- mfa-enabled-for-iam-akses konsol
- mq-active-broker-ldap-otentikasi
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-upgrade diaktifkan
- mq-broker-general-logging-diaktifkan
- mq-cloudwatch-audit-log-diaktifkan
- mq-rabbit-deployment-mode
- msk-cluster-public-access-dinonaktifkan
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-internal-scheme-check
- nlb-logging-enabled

- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-toleransi
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-pemeriksaan enkripsi-
- opensearch-primary-node-fault-toleransi
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-aurora-postgresql-logske cloudwatch
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat

- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-diaktifkan
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-serverless-default-admin-periksa
- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi

- redshift-serverless-publish-logske cloudwatch
- redshift-serverless-workgroup-no-akses publik
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-ember dengan tag
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- -dibuat last-backup-recovery-point

- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-ditandai
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-instance-root-akses-cek
- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-akses

- ssm-automation-block-public-berbagi
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled

- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong

Wilayah Asia Pasifik (Malaysia)

Asia Pasifik (Malaysia)

- account-part-of-organizations
- acm-certificate-expiration-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pemeriksaan-pengalihan
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launch-config-public-ip-dinonaktifkan
- cloudformation-stack-drift-detection-periksa
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted

- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- cw-loggroup-retention-period-periksa
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-public-restorable-periksa
- ec2- ebs-encryption-by-default
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required

- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- -eni security-group-attached-to
- ec2-stopped-instance
- ec2- volume-inuse-check
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan
- terlampir eip
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-periksa
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-kerberos-enabled
- emr-master-no-public-ip
- volume terenkripsi

- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- kms-cmk-not-scheduled-untuk-penghapusan
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-diaktifkan
- no-unrestricted-route-to-igw
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted

- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-periksa
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- tag yang dibutuhkan
- restricted-incoming-traffic
- s3- account-level-public-access -blok-periodik
- s3- bucket-blacklisted-actions-prohibited
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub-enabled
- service-vpc-endpoint-enabled

- sns-encrypted-kms
- ssm-document-not-public
- subnet-auto-assign-public-ip-dinonaktifkan
- vpc-default-security-group-tertutup
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan

Wilayah Asia Pasifik (Melbourne)

Asia Pasifik (Melbourne)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan
- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pemeriksaan-pengalihan
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled

- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-tidak-kosong
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-penyimpanan
- appconfig-hosted-configuration-version-deskripsi
- approved-amis-by-id
- approved-amis-by-tag
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template

- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapusan-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat

- cognito-identity-pool-unauth-akses-cek
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- diaktifkan client-vpn-connection-log

- ec2- client-vpn-endpoint-tagged
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- diaktifkan enis-source-destination-check
- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -dibuat last-backup-recovery-point
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- prefix-list-tagged
- ec2- resources-in-logically-air -gapped-lemari besi
- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged

- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan
- terlampir eip

- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan
- elasticache-redis-cluster-automatic-backup-periksa
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-block-public-access
- emr-kerberos-enabled
- emr-security-configuration-encryption-istirahat
- emr-security-configuration-encryption-transit
- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- fsx-last-backup-recovery-point-dibuat
- fsx-lustre-copy-tagsuntuk cadangan

- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-deployment-type-periksa
- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-diaktifkan
- iam-password-policy
- iam-root-access-key-periksa
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik

- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- mariadb-publish-logs-to-cloudwatch-log
- mq-active-broker-ldap-otentikasi
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-upgrade diaktifkan
- mq-broker-general-logging-diaktifkan
- mq-cloudwatch-audit-log-diaktifkan
- msk-cluster-public-access-dinonaktifkan
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-internal-scheme-check

- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted

- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-diaktifkan
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check

- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-ember dengan tag
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-hitungan contoh
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-akses
- ssm-automation-logging-enabled
- ssm-document-not-public

- ssm-document-tagged
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-sg-port-restriction-periksa
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-kosong
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong

Wilayah Asia Pasifik (Mumbai)

Asia Pasifik (Mumbai)

- access-keys-rotated

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pengalihan-periksa
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-penghapusan-diaktifkan
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-diaktifkan
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-tidak-kosong

- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-penyimpanan
- appconfig-hosted-configuration-version-deskripsi
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-penerusan
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-default-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-akses
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf

- appsync-authorization-check
- appsync-cache-encryption-at-istirahat
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-istirahat
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapus-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi
- batch-compute-environment-enabled

- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-diaktifkan
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-periksa
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan

- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-periksa
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- codedeploy-auto-rollback-monitor-diaktifkan
- codedeploy-deployment-group-auto-rollback-diaktifkan
- codedeploy-deployment-group-outdated-instances-pembaruan
- codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-akses-cek
- cognito-user-pool-advanced-keamanan diaktifkan
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-Terlampir
- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-tingkatkan periksa

- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-diaktifkan
- dms-neptune-iam-authorization-diaktifkan
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-diaktifkan
- docdb-cluster-backup-retention-periksa
- docdb-cluster-deletion-protection-diaktifkan
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-dilarang
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target
- ebs-optimized-instance

- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- diaktifkan client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -semua client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- diaktifkan enis-source-destination-check
- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -dibuat last-backup-recovery-point
- ec2- 2-periksa launch-template-imdsv
- ec2- launch-template-public-ip -dinonaktifkan
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -periksa managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target

- ec2- network-insights-access-scope -analisis ditandai
- ec2- -ditandai network-insights-access-scope
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- resources-in-logically-air -gapped-lemari besi
- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2- security-group-attached-to -eni-periodik
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan
- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access

- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi
- ecs-task-definition-memory-batas-keras
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-pengguna
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan
- terlampir eip
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versi
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan

- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan
- elasticache-repl-grp-encrypted-saat istirahat
- elasticache-repl-grp-encrypted-dalam transit
- elasticache-repl-grp-redis-auth-diaktifkan
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-logs-to-jam tangan awan
- elastic-beanstalk-managed-updates-diaktifkan
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -periksa predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya

- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-istirahat
- emr-security-configuration-encryption-transit
- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan
- fis-experiment-template-log-konfigurasi-ada
- fis-experiment-template-tagged
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- fsx-last-backup-recovery-point-dibuat
- fsx-lustre-copy-tagsuntuk cadangan
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-audit-log-dikonfigurasi
- fsx-windows-deployment-type-periksa
- glb-listener-tagged
- global-endpoint-event-replication-diaktifkan
- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan

- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-tindakan
- iam-external-access-analyzer-diaktifkan
- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa
- iam-root-access-key-periksa
- iam-user-group-membership-periksa
- iam-user-mfa-enabled
- iam-user-no-policies-periksa
- iam-user-unused-credentials-periksa
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-diaktifkan
- instances-in-vpc

- internet-gateway-authorized-vpc-hanya
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iot-authorizer-token-signing-diaktifkan
- ivs-channel-playback-authorization-diaktifkan
- ivs-channel-tagged
- ivs-playback-key-pair-ditandai
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc

- lambda-vpc-multi-az-periksa
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-penemuan-cek
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-log
- mfa-enabled-for-iam-akses konsol
- mq-active-broker-ldap-otentikasi
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade diaktifkan
- mq-auto-minor-version-upgrade diaktifkan
- mq-broker-general-logging-diaktifkan
- mq-cloudwatch-audit-logging-diaktifkan
- mq-cloudwatch-audit-log-diaktifkan
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-dinonaktifkan
- msk-connect-connector-logging-diaktifkan
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-periksa
- neptune-cluster-cloudwatch-log-ekspor diaktifkan
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-diaktifkan

- neptune-cluster-encrypted
- neptune-cluster-iam-database-otentikasi
- neptune-cluster-multi-az-diaktifkan
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-dilarang
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-cross-zone-load-menyeimbangkan diaktifkan
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-toleransi
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-pemeriksaan enkripsi-
- opensearch-primary-node-fault-toleransi
- opensearch-update-check
- rabbit-mq-supported-version

- rds-aurora-mysql-audit-logging-diaktifkan
- rds-aurora-postgresql-logske cloudwatch
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit

- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-diaktifkan
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-serverless-default-admin-periksa
- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi
- redshift-serverless-publish-logske cloudwatch
- redshift-serverless-workgroup-encrypted-dalam transit
- redshift-serverless-workgroup-no-akses publik
- redshift-serverless-workgroup-routes-dalam-vpc
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- s3 -aturan-periksa express-dir-bucket-lifecycle
- s3- -hanya access-point-in-vpc

- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-ember dengan tag
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -gapped-lemari besi
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-ditandai
- sagemaker-domain-in-vpc

- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-instance-root-akses-cek
- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub diaktifkan
- security-account-information-provided
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notifikasi-diaktifkan
- sns-topic-no-public-akses
- sqs-queue-no-public-akses
- ssm-automation-block-public-berbagi
- ssm-automation-logging-enabled
- ssm-document-not-public

- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-dibuat
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-rencana cadangan
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-peering-dns-resolution-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled

- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-kosong
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong
- workspaces-root-volume-encryption-diaktifkan
- workspaces-user-volume-encryption-diaktifkan

Wilayah Asia Pasifik (Osaka)

Asia Pasifik (Osaka)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan
- active-mq-supported-version
- alb-desync-mode-check
- alb-internal-scheme-check
- alb-listener-tagged
- amplify-app-branch-auto-penghapusan-diaktifkan
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-diaktifkan
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi

- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-tidak-kosong
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-penyimpanan
- appconfig-hosted-configuration-version-deskripsi
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-penerusan
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-default-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag

- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-istirahat
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-istirahat
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapus-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi

- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-periksa
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-envvar-awscred-periksa

- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- codedeploy-auto-rollback-monitor-diaktifkan
- codedeploy-deployment-group-auto-rollback-diaktifkan
- codedeploy-deployment-group-outdated-instances-pembaruan
- codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan
- cognito-identity-pool-unauth-akses-cek
- cognito-user-pool-advanced-keamanan diaktifkan
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-tingkatkan periksa
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-diaktifkan
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-tagged
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan

- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- diaktifkan client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- diaktifkan enis-source-destination-check
- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -dibuat last-backup-recovery-point

- ec2- 2-periksa launch-template-imdsv
- ec2- launch-template-public-ip -dinonaktifkan
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- network-insights-access-scope -analisis ditandai
- ec2- -ditandai network-insights-access-scope
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- resources-in-logically-air -gapped-lemari besi
- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan

- ecr-repository-cmk-encryption-diaktifkan
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan
- terlampir eip
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted

- elasticache-automatic-backup-check-diaktifkan
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan
- elasticache-repl-grp-encrypted-saat istirahat
- elasticache-repl-grp-encrypted-dalam transit
- elasticache-repl-grp-redis-auth-diaktifkan
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-logs-to-jam tangan awan
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -periksa predefined-security-policy-ssl
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-logging-enabled
- emr-block-public-access
- emr-kerberos-enabled
- emr-security-configuration-encryption-istirahat
- emr-security-configuration-encryption-transit
- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan
- fms-shield-resource-policy-periksa

- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- fsx-last-backup-recovery-point-dibuat
- fsx-lustre-copy-tagsuntuk cadangan
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-audit-log-dikonfigurasi
- fsx-windows-deployment-type-periksa
- glb-listener-tagged
- global-endpoint-event-replication-diaktifkan
- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-tindakan
- iam-external-access-analyzer-diaktifkan

- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa
- iam-root-access-key-periksa
- iam-user-group-membership-periksa
- iam-user-mfa-enabled
- iam-user-no-policies-periksa
- iam-user-unused-credentials-periksa
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-diaktifkan
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check

- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- macie-auto-sensitive-data-penemuan-cek
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-log
- mfa-enabled-for-iam-akses konsol
- mq-active-broker-ldap-otentikasi
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade diaktifkan
- mq-auto-minor-version-upgrade diaktifkan
- mq-broker-general-logging-diaktifkan
- mq-cloudwatch-audit-logging-diaktifkan
- mq-cloudwatch-audit-log-diaktifkan
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-dinonaktifkan
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-periksa
- neptune-cluster-cloudwatch-log-ekspor diaktifkan
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-diaktifkan
- neptune-cluster-encrypted
- neptune-cluster-iam-database-otentikasi

- neptune-cluster-multi-az-diaktifkan
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-dilarang
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-cross-zone-load-menyeimbangkan diaktifkan
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-toleransi
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-pemeriksaan enkripsi-
- opensearch-primary-node-fault-toleransi
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-aurora-postgresql-logske cloudwatch

- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted

- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-diaktifkan
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled

- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-ember dengan tag
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -gapped-lemari besi
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-ditandai
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi

- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-instance-root-akses-cek
- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub diaktifkan
- security-account-information-provided
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notifikasi-diaktifkan
- sns-topic-no-public-akses
- sqs-queue-no-public-akses
- ssm-automation-block-public-berbagi
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged

- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-dibuat
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-rencana cadangan
- vpc-default-security-group-tertutup
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-peering-dns-resolution-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong

Wilayah Asia Pasifik (Seoul)

Asia Pasifik (Seoul)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check

- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pengalihan-periksa
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-penghapusan-diaktifkan
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-diaktifkan
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-tidak-kosong
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-environment-description

- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-penyimpanan
- appconfig-hosted-configuration-version-deskripsi
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-penerusan
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-default-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-istirahat
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description

- athena-workgroup-encrypted-at-istirahat
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapus-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged

- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-diaktifkan
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-periksa
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-periksa
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa

- codebuild-report-group-encrypted-saat istirahat
- codedeploy-auto-rollback-monitor-diaktifkan
- codedeploy-deployment-group-auto-rollback-diaktifkan
- codedeploy-deployment-group-outdated-instances-pembaruan
- codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-user-pool-advanced-keamanan diaktifkan
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-pembuatan profil
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-Terlampir
- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-tingkatkan periksa
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-diaktifkan
- dms-neptune-iam-authorization-diaktifkan
- dms-redis-tls-enabled
- dms-replication-not-public

- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-diaktifkan
- docdb-cluster-backup-retention-periksa
- docdb-cluster-deletion-protection-diaktifkan
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-dilarang
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- diaktifkan client-vpn-connection-log

- ec2- client-vpn-endpoint-tagged
- ec2- -semua client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -dibuat last-backup-recovery-point
- ec2- 2-periksa launch-template-imdsv
- ec2- launch-template-public-ip -dinonaktifkan
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -periksa managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- network-insights-access-scope -analisis ditandai
- ec2- -ditandai network-insights-access-scope
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- resources-in-logically-air -gapped-lemari besi

- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2- security-group-attached-to -eni-periodik
- ec2- - spot-fleet-request-ct encryption-at-rest
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan
- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi
- ecs-task-definition-memory-batas-keras

- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-pengguna
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan
- terlampir eip
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versi
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan
- elasticache-repl-grp-encrypted-saat istirahat

- elasticache-repl-grp-encrypted-dalam transit
- elasticache-repl-grp-redis-auth-diaktifkan
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-logs-to-jam tangan awan
- elastic-beanstalk-managed-updates-diaktifkan
- elbv2- acm-certificate-required
- elbv2-multiple-az
- elbv2- -periksa predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-istirahat
- emr-security-configuration-encryption-transit
- volume terenkripsi

- event-data-store-cmk-enkripsi diaktifkan
- fis-experiment-template-log-konfigurasi-ada
- fis-experiment-template-tagged
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- fsx-last-backup-recovery-point-dibuat
- fsx-lustre-copy-tagsuntuk cadangan
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-audit-log-dikonfigurasi
- fsx-windows-deployment-type-periksa
- glb-listener-tagged
- global-endpoint-event-replication-diaktifkan
- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled

- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-tindakan
- iam-external-access-analyzer-diaktifkan
- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa
- iam-root-access-key-periksa
- iam-user-group-membership-periksa
- iam-user-mfa-enabled
- iam-user-no-policies-periksa
- iam-user-unused-credentials-periksa
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-diaktifkan
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged

- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iot-authorizer-token-signing-diaktifkan
- ivs-channel-playback-authorization-diaktifkan
- ivs-channel-tagged
- ivs-playback-key-pair-ditandai
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-penemuan-cek
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-log

- mfa-enabled-for-iam-akses konsol
- mq-active-broker-ldap-otentikasi
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade diaktifkan
- mq-auto-minor-version-upgrade diaktifkan
- mq-broker-general-logging-diaktifkan
- mq-cloudwatch-audit-logging-diaktifkan
- mq-cloudwatch-audit-log-diaktifkan
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-periksa
- neptune-cluster-cloudwatch-log-ekspor diaktifkan
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-diaktifkan
- neptune-cluster-encrypted
- neptune-cluster-iam-database-otentikasi
- neptune-cluster-multi-az-diaktifkan
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-dilarang
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh

- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-cross-zone-load-menyeimbangkan diaktifkan
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-toleransi
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-pemeriksaan enkripsi-
- opensearch-primary-node-fault-toleransi
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-aurora-postgresql-logske cloudwatch
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-enhanced-monitoring-enabled

- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az

- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-serverless-default-admin-periksa
- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi
- redshift-serverless-publish-logske cloudwatch
- redshift-serverless-workgroup-encrypted-dalam transit
- redshift-serverless-workgroup-no-akses publik
- redshift-serverless-workgroup-routes-dalam-vpc
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif

- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-ember dengan tag
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -gapped-lemari besi
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-ditandai
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-instance-root-akses-cek

- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notifikasi-diaktifkan
- sns-topic-no-public-akses
- sqs-queue-no-public-akses
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged

- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-dibuat
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-rencana cadangan
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-peering-dns-resolution-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-kosong
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong
- workspaces-root-volume-encryption-diaktifkan
- workspaces-user-volume-encryption-diaktifkan

Wilayah Asia Pasifik (Singapura)

Asia Pasifik (Singapura)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged

- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pengalihan-periksa
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-penghapusan-diaktifkan
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-diaktifkan
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-tidak-kosong
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm

- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-penyimpanan
- appconfig-hosted-configuration-version-deskripsi
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-penerusan
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-default-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-akses
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf

- appsync-authorization-check
- appsync-cache-encryption-at-istirahat
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-istirahat
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-pencatatan
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapus-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi
- batch-compute-environment-enabled

- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-diaktifkan
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-periksa
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan

- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-periksa
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- codedeploy-auto-rollback-monitor-diaktifkan
- codedeploy-deployment-group-auto-rollback-diaktifkan
- codedeploy-deployment-group-outdated-instances-pembaruan
- codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-akses-cek
- cognito-user-pool-advanced-keamanan diaktifkan
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-pembuatan profil
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-Terlampir
- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled

- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-tingkatkan periksa
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-diaktifkan
- dms-neptune-iam-authorization-diaktifkan
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-pencatatan
- dms-replication-task-tagged
- dms-replication-task-targetdb-pencatatan
- docdb-cluster-audit-logging-diaktifkan
- docdb-cluster-backup-retention-periksa
- docdb-cluster-deletion-protection-diaktifkan
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-dilarang
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled

- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- diaktifkan client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -semua client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- diaktifkan enis-source-destination-check
- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -dibuat last-backup-recovery-point
- ec2- 2-periksa launch-template-imdsv
- ec2- launch-template-public-ip -dinonaktifkan
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required

- ec2- -periksa managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- network-insights-access-scope -analisis ditandai
- ec2- -ditandai network-insights-access-scope
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2- resources-in-logically-air -gapped-lemari besi
- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2- security-group-attached-to -eni-periodik
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan
- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi

- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi
- ecs-task-definition-memory-batas-keras
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-pengguna
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan
- terlampir eip
- eks-cluster-logging-enabled
- eks-cluster-log-enabled

- eks-cluster-oldest-supported-versi
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan
- elasticache-repl-grp-encrypted-saat istirahat
- elasticache-repl-grp-encrypted-dalam transit
- elasticache-repl-grp-redis-auth-diaktifkan
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-logs-to-jam tangan awan
- elastic-beanstalk-managed-updates-diaktifkan
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -periksa predefined-security-policy-ssl
- elb-acm-certificate-required

- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-istirahat
- emr-security-configuration-encryption-transit
- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-konfigurasi-ada
- fis-experiment-template-tagged
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-dibuat

- fsx-lustre-copy-tagsuntuk cadangan
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-audit-log-dikonfigurasi
- fsx-windows-deployment-type-periksa
- glb-listener-tagged
- global-endpoint-event-replication-diaktifkan
- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-tindakan
- iam-external-access-analyzer-diaktifkan
- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa

- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa
- iam-root-access-key-periksa
- iam-user-group-membership-periksa
- iam-user-mfa-enabled
- iam-user-no-policies-periksa
- iam-user-unused-credentials-periksa
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-diaktifkan
- inspector-lambda-standard-scan-diaktifkan
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged

- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iot-authorizer-token-signing-diaktifkan
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-penemuan-cek
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-log
- mfa-enabled-for-iam-akses konsol
- mq-active-broker-ldap-otentikasi
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade diaktifkan
- mq-auto-minor-version-upgrade diaktifkan
- mq-broker-general-logging-diaktifkan
- mq-cloudwatch-audit-logging-diaktifkan

- mq-cloudwatch-audit-log-diaktifkan
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-dinonaktifkan
- msk-connect-connector-logging-diaktifkan
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-periksa
- neptune-cluster-cloudwatch-log-ekspor diaktifkan
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-diaktifkan
- neptune-cluster-encrypted
- neptune-cluster-iam-database-otentikasi
- neptune-cluster-multi-az-diaktifkan
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-dilarang
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-cross-zone-load-menyeimbangkan diaktifkan
- nlb-internal-scheme-check

- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-toleransi
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-pemeriksaan enkripsi-
- opensearch-primary-node-fault-toleransi
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-aurora-postgresql-logske cloudwatch
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-db-security-group-tidak diizinkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa

- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-diaktifkan
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan

- redshift-require-tls-ssl
- redshift-serverless-default-admin-periksa
- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi
- redshift-serverless-publish-logske cloudwatch
- redshift-serverless-workgroup-encrypted-dalam transit
- redshift-serverless-workgroup-no-akses publik
- redshift-serverless-workgroup-routes-dalam-vpc
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled

- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -gapped-lemari besi
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-ditandai
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-instance-root-akses-cek
- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa

- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub diaktifkan
- security-account-information-provided
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notifikasi-diaktifkan
- sns-topic-no-public-akses
- sqs-queue-no-public-akses
- ssm-automation-block-public-berbagi
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description

- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-dibuat
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-rencana cadangan
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-peering-dns-resolution-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-kosong
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong
- workspaces-root-volume-encryption-diaktifkan
- workspaces-user-volume-encryption-diaktifkan

Wilayah Asia Pasifik (Sydney)

Asia Pasifik (Sydney)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check

- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pengalihan-periksa
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-penghapusan-diaktifkan
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-diaktifkan
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-tidak-kosong
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-environment-description

- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-penyimpanan
- appconfig-hosted-configuration-version-deskripsi
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-penerusan
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-default-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-akses
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check

- appsync-cache-encryption-at-istirahat
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-istirahat
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapus-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi
- batch-compute-environment-enabled
- batch-compute-environment-managed

- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-diaktifkan
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-periksa
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-artifact-encryption

- codebuild-project-environment-privileged-periksa
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- codedeploy-auto-rollback-monitor-diaktifkan
- codedeploy-deployment-group-auto-rollback-diaktifkan
- codedeploy-deployment-group-outdated-instances-pembaruan
- codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-akses-cek
- cognito-user-pool-advanced-keamanan diaktifkan
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-pembuatan profil
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-Terlampir
- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption

- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-tingkatkan periksa
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-diaktifkan
- dms-neptune-iam-authorization-diaktifkan
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-diaktifkan
- docdb-cluster-backup-retention-periksa
- docdb-cluster-deletion-protection-diaktifkan
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-dilarang
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check

- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- diaktifkan client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -semua client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- diaktifkan enis-source-destination-check
- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -dibuat last-backup-recovery-point
- ec2- 2-periksa launch-template-imdsv
- ec2- launch-template-public-ip -dinonaktifkan
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required

- ec2- -periksa managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- network-insights-access-scope -analisis ditandai
- ec2- -ditandai network-insights-access-scope
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2- resources-in-logically-air -gapped-lemari besi
- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2- security-group-attached-to -eni-periodik
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan
- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi

- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi
- ecs-task-definition-memory-batas-keras
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-pengguna
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan
- terlampir eip
- eks-cluster-logging-enabled
- eks-cluster-log-enabled

- eks-cluster-oldest-supported-versi
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan
- elasticache-repl-grp-encrypted-saat istirahat
- elasticache-repl-grp-encrypted-dalam transit
- elasticache-repl-grp-redis-auth-diaktifkan
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-logs-to-jam tangan awan
- elastic-beanstalk-managed-updates-diaktifkan
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -periksa predefined-security-policy-ssl
- elb-acm-certificate-required

- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-istirahat
- emr-security-configuration-encryption-transit
- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-konfigurasi-ada
- fis-experiment-template-tagged
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-dibuat

- fsx-lustre-copy-tagsuntuk cadangan
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-audit-log-dikonfigurasi
- fsx-windows-deployment-type-periksa
- glb-listener-tagged
- global-endpoint-event-replication-diaktifkan
- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-tindakan
- iam-external-access-analyzer-diaktifkan
- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa

- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa
- iam-root-access-key-periksa
- iam-user-group-membership-periksa
- iam-user-mfa-enabled
- iam-user-no-policies-periksa
- iam-user-unused-credentials-periksa
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-diaktifkan
- inspector-lambda-standard-scan-diaktifkan
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged

- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-diaktifkan
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-penemuan-cek
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-log
- mfa-enabled-for-iam-akses konsol
- mq-active-broker-ldap-otentikasi
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade diaktifkan

- mq-auto-minor-version-upgrade diaktifkan
- mq-broker-general-logging-diaktifkan
- mq-cloudwatch-audit-logging-diaktifkan
- mq-cloudwatch-audit-log-diaktifkan
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-dinonaktifkan
- msk-connect-connector-logging-diaktifkan
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-periksa
- neptune-cluster-cloudwatch-log-ekspor diaktifkan
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-diaktifkan
- neptune-cluster-encrypted
- neptune-cluster-iam-database-otentikasi
- neptune-cluster-multi-az-diaktifkan
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-dilarang
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong

- netfw-subnet-change-protection-diaktifkan
- nlb-cross-zone-load-menyeimbangkan diaktifkan
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-toleransi
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-pemeriksaan enkripsi-
- opensearch-primary-node-fault-toleransi
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-aurora-postgresql-logske cloudwatch
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-db-security-group-tidak diizinkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa

- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-diaktifkan
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az

- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-serverless-default-admin-periksa
- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi
- redshift-serverless-publish-logske cloudwatch
- redshift-serverless-workgroup-encrypted-dalam transit
- redshift-serverless-workgroup-no-akses publik
- redshift-serverless-workgroup-routes-dalam-vpc
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif

- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -gapped-lemari besi
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-ditandai
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-instance-root-akses-cek

- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notifikasi-diaktifkan
- sns-topic-no-public-akses
- sqs-queue-no-public-akses
- ssm-automation-block-public-berbagi
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged

- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-dibuat
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-rencana cadangan
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-peering-dns-resolution-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-kosong
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong
- workspaces-root-volume-encryption-diaktifkan
- workspaces-user-volume-encryption-diaktifkan

Wilayah Asia Pasifik (Taipei)

Asia Pasifik (Taipei)

- acm-certificate-expiration-check

- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pengalihan-periksa
- alb-waf-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-mysql-backtracking-enabled
- cloudformation-stack-drift-detection-periksa
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- cw-loggroup-retention-period-periksa
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-encryption-enabled
- ebs-snapshot-public-restorable-periksa
- ec2- ebs-encryption-by-default
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed

- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2-stopped-instance
- terlampir eip
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- volume terenkripsi
- incoming-ssh-disabled
- instances-in-vpc
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-diaktifkan
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited

- rds-snapshot-encrypted
- rds-storage-encrypted
- tag yang dibutuhkan
- restricted-incoming-traffic
- s3- account-level-public-access -blok-periodik
- s3- bucket-blacklisted-actions-prohibited
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3- bucket-versioning-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- subnet-auto-assign-public-ip-dinonaktifkan
- vpc-default-security-group-tertutup
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-terowongan

Wilayah Asia Pasifik (Thailand)

Asia Pasifik (Thailand)

- account-part-of-organizations
- acm-certificate-expiration-check

- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pengalihan-periksa
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launch-config-public-ip-dinonaktifkan
- cloudformation-stack-drift-detection-periksa
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- cw-loggroup-retention-period-periksa
- db-instance-backup-enabled

- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-public-restorable-periksa
- ec2- ebs-encryption-by-default
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- -eni security-group-attached-to
- ec2-stopped-instance
- ec2- volume-inuse-check
- ecs-task-definition-user-for-host-mode-check

- efs-encrypted-check
- efs-in-backup-plan
- terlampir eip
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-periksa
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-kerberos-enabled
- emr-master-no-public-ip
- volume terenkripsi
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- kms-cmk-not-scheduled-untuk-penghapusan
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check

- lambda-inside-vpc
- multi-region-cloud-trail-diaktifkan
- no-unrestricted-route-to-igw
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- tag yang dibutuhkan
- restricted-incoming-traffic
- s3- account-level-public-access -blok-periodik
- s3- bucket-blacklisted-actions-prohibited
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled

- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- subnet-auto-assign-public-ip-dinonaktifkan
- vpc-default-security-group-tertutup
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-terowongan

Wilayah Asia Pasifik (Tokyo)

Asia Pasifik (Tokyo)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan

- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pengalihan-periksa
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-penghapusan-diaktifkan
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-diaktifkan
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-tidak-kosong
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged

- appconfig-freeform-profile-config-penyimpanan
- appconfig-hosted-configuration-version-deskripsi
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-penerusan
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-default-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-akses
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-istirahat
- appsync-logging-enabled

- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-istirahat
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapus-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled

- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-diaktifkan
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-periksa
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-periksa
- codebuild-project-envvar-awscred-periksa

- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- codedeploy-auto-rollback-monitor-diaktifkan
- codedeploy-deployment-group-auto-rollback-diaktifkan
- codedeploy-deployment-group-outdated-instances-pembaruan
- codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-akses-cek
- cognito-user-pool-advanced-keamanan diaktifkan
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-pembuatan profil
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-Terlampir
- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy

- desired-instance-type
- dms-auto-minor-version-tingkatkan periksa
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-diaktifkan
- dms-neptune-iam-authorization-diaktifkan
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-diaktifkan
- docdb-cluster-backup-retention-periksa
- docdb-cluster-deletion-protection-diaktifkan
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-dilarang
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat

- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- diaktifkan client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -semua client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- diaktifkan enis-source-destination-check
- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -dibuat last-backup-recovery-point
- ec2- 2-periksa launch-template-imdsv
- ec2- launch-template-public-ip -dinonaktifkan
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -periksa managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted

- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- network-insights-access-scope -analisis ditandai
- ec2- -ditandai network-insights-access-scope
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2- resources-in-logically-air -gapped-lemari besi
- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2- security-group-attached-to -eni-periodik
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan
- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan

- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi
- ecs-task-definition-memory-batas-keras
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-pengguna
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan
- terlampir eip
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versi
- eks-cluster-secrets-encrypted

- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan
- elasticache-repl-grp-encrypted-saat istirahat
- elasticache-repl-grp-encrypted-dalam transit
- elasticache-repl-grp-redis-auth-diaktifkan
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-logs-to-jam tangan awan
- elastic-beanstalk-managed-updates-diaktifkan
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -periksa predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa

- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-istirahat
- emr-security-configuration-encryption-transit
- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-konfigurasi-ada
- fis-experiment-template-tagged
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- fsx-last-backup-recovery-point-dibuat
- fsx-lustre-copy-tagsuntuk cadangan
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan

- fsx-windows-audit-log-dikonfigurasi
- fsx-windows-deployment-type-periksa
- glb-listener-tagged
- global-endpoint-event-replication-diaktifkan
- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-tindakan
- iam-external-access-analyzer-diaktifkan
- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa

- iam-root-access-key-periksa
- iam-user-group-membership-periksa
- iam-user-mfa-enabled
- iam-user-no-policies-periksa
- iam-user-unused-credentials-periksa
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-diaktifkan
- inspector-lambda-standard-scan-diaktifkan
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-diaktifkan
- ivs-channel-playback-authorization-diaktifkan

- ivs-channel-tagged
- ivs-playback-key-pair-ditandai
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-penemuan-cek
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-log
- mfa-enabled-for-iam-akses konsol
- mq-active-broker-ldap-otentikasi
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade diaktifkan
- mq-auto-minor-version-upgrade diaktifkan
- mq-broker-general-logging-diaktifkan
- mq-cloudwatch-audit-logging-diaktifkan

- mq-cloudwatch-audit-log-diaktifkan
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-dinonaktifkan
- msk-connect-connector-logging-diaktifkan
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-periksa
- neptune-cluster-cloudwatch-log-ekspor diaktifkan
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-diaktifkan
- neptune-cluster-encrypted
- neptune-cluster-iam-database-otentikasi
- neptune-cluster-multi-az-diaktifkan
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-dilarang
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-cross-zone-load-menyeimbangkan diaktifkan
- nlb-internal-scheme-check

- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-toleransi
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-pemeriksaan enkripsi-
- opensearch-primary-node-fault-toleransi
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-aurora-postgresql-logske cloudwatch
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-db-security-group-tidak diizinkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa

- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-diaktifkan
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan

- redshift-require-tls-ssl
- redshift-serverless-default-admin-periksa
- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi
- redshift-serverless-publish-logske cloudwatch
- redshift-serverless-workgroup-encrypted-dalam transit
- redshift-serverless-workgroup-no-akses publik
- redshift-serverless-workgroup-routes-dalam-vpc
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- s3 -aturan-periksa express-dir-bucket-lifecycle
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited

- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -gapped-lemari besi
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-ditandai
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-instance-root-akses-cek
- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check

- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub diaktifkan
- security-account-information-provided
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notifikasi-diaktifkan
- sns-topic-no-public-akses
- sqs-queue-no-public-akses
- ssm-automation-block-public-berbagi
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged

- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-dibuat
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-rencana cadangan
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-peering-dns-resolution-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-kosong
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong
- workspaces-root-volume-encryption-diaktifkan
- workspaces-user-volume-encryption-diaktifkan

Wilayah Kanada (Pusat)

Kanada (Pusat)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged

- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pengalihan-periksa
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-penghapusan-diaktifkan
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-diaktifkan
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-tidak-kosong
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm

- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-penyimpanan
- appconfig-hosted-configuration-version-deskripsi
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-penerusan
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-default-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-istirahat
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description

- athena-workgroup-description
- athena-workgroup-encrypted-at-istirahat
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapus-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template

- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-diaktifkan
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-periksa
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-periksa
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi

- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- codedeploy-auto-rollback-monitor-diaktifkan
- codedeploy-deployment-group-auto-rollback-diaktifkan
- codedeploy-deployment-group-outdated-instances-pembaruan
- codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-akses-cek
- cognito-user-pool-advanced-keamanan diaktifkan
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-pembuatan profil
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-Terlampir
- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-tingkatkan periksa
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-diaktifkan
- dms-neptune-iam-authorization-diaktifkan

- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-pencatatan
- dms-replication-task-tagged
- dms-replication-task-targetdb-pencatatan
- docdb-cluster-audit-logging-diaktifkan
- docdb-cluster-backup-retention-periksa
- docdb-cluster-deletion-protection-diaktifkan
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-dilarang
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged

- ec2- carrier-gateway-tagged
- ec2- diaktifkan client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -semua client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- diaktifkan enis-source-destination-check
- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -dibuat last-backup-recovery-point
- ec2- 2-periksa launch-template-imdsv
- ec2- launch-template-public-ip -dinonaktifkan
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -periksa managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- network-insights-access-scope -analisis ditandai
- ec2- -ditandai network-insights-access-scope
- ec2- network-insights-path-tagged

- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- resources-in-logically-air -gapped-lemari besi
- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2- security-group-attached-to -eni-periodik
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan
- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets

- ecs-task-definition-log-konfigurasi
- ecs-task-definition-memory-batas-keras
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-pengguna
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan
- terlampir eip
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versi
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-periksa

- elasticache-repl-grp-auto-failover-diaktifkan
- elasticache-repl-grp-encrypted-saat istirahat
- elasticache-repl-grp-encrypted-dalam transit
- elasticache-repl-grp-redis-auth-diaktifkan
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-logs-to-jam tangan awan
- elastic-beanstalk-managed-updates-diaktifkan
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -periksa predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip

- emr-security-configuration-encryption-istirahat
- emr-security-configuration-encryption-transit
- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan
- fis-experiment-template-log-konfigurasi-ada
- fis-experiment-template-tagged
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- fsx-last-backup-recovery-point-dibuat
- fsx-lustre-copy-tagsuntuk cadangan
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-audit-log-dikonfigurasi
- fsx-windows-deployment-type-periksa
- glb-listener-tagged
- global-endpoint-event-replication-diaktifkan
- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled

- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-tindakan
- iam-external-access-analyzer-diaktifkan
- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa
- iam-root-access-key-periksa
- iam-user-group-membership-periksa
- iam-user-mfa-enabled
- iam-user-no-policies-periksa
- iam-user-unused-credentials-periksa
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-diaktifkan
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged

- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iot-authorizer-token-signing-diaktifkan
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-penemuan-cek
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-log
- mfa-enabled-for-iam-akses konsol
- mq-active-broker-ldap-otentikasi
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs

- mq-automatic-minor-version-upgrade diaktifkan
- mq-auto-minor-version-upgrade diaktifkan
- mq-broker-general-logging-diaktifkan
- mq-cloudwatch-audit-logging-diaktifkan
- mq-cloudwatch-audit-log-diaktifkan
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-dinonaktifkan
- msk-connect-connector-logging-diaktifkan
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-periksa
- neptune-cluster-cloudwatch-log-ekspor diaktifkan
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-diaktifkan
- neptune-cluster-encrypted
- neptune-cluster-iam-database-otentikasi
- neptune-cluster-multi-az-diaktifkan
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-dilarang
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait

- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-cross-zone-load-menyeimbangkan diaktifkan
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-toleransi
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-pemeriksaan enkripsi-
- opensearch-primary-node-fault-toleransi
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-aurora-postgresql-logske cloudwatch
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa

- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-diaktifkan
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az

- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-serverless-default-admin-periksa
- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi
- redshift-serverless-publish-logske cloudwatch
- redshift-serverless-workgroup-encrypted-dalam transit
- redshift-serverless-workgroup-no-akses publik
- redshift-serverless-workgroup-routes-dalam-vpc
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif

- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -gapped-lemari besi
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-ditandai
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-instance-root-akses-cek

- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notifikasi-diaktifkan
- sns-topic-no-public-akses
- sqs-queue-no-public-akses
- ssm-automation-block-public-berbagi
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged

- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-dibuat
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-rencana cadangan
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-peering-dns-resolution-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-kosong
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong
- workspaces-root-volume-encryption-diaktifkan
- workspaces-user-volume-encryption-diaktifkan

Wilayah Kanada Barat (Calgary)

Kanada Barat (Calgary)

- account-part-of-organizations

- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pengalihan-periksa
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm
- approved-amis-by-id
- approved-amis-by-tag
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launch-config-public-ip-dinonaktifkan
- batch-scheduling-policy-tagged
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check

- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- cognito-user-pool-tagged
- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed

- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- prefix-list-tagged
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- -ditandai transit-gateway-multicast-domain
- ecr-repository-tagged
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan
- terlampir eip
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-periksa
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-security-configuration-encryption-istirahat
- emr-security-configuration-encryption-transit

- volume terenkripsi
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- incoming-ssh-disabled
- instances-in-vpc
- kms-cmk-not-scheduled-untuk-penghapusan
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-diaktifkan
- nlb-internal-scheme-check
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check

- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- tag yang dibutuhkan
- restricted-incoming-traffic
- s3- account-level-public-access -blok-periodik
- s3- bucket-blacklisted-actions-prohibited
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-bucket-tagged
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk

- Securityhub-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-tagged
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-tertutup
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan

Wilayah Tiongkok (Beijing)

Tiongkok (Beijing)

- access-keys-rotated
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pengalihan-periksa
- alb-waf-enabled
- api-gwv2- access-logs-enabled

- api-gwv2- authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-istirahat
- athena-workgroup-logging-enabled
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- beanstalk-enhanced-health-reporting-diaktifkan
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-periksa
- cloudformation-stack-notification-check
- cloudfront-s3- origin-non-existent-bucket
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited

- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-environment-privileged-periksa
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-periksa
- datasync-task-logging-enabled
- dax-encryption-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-tingkatkan periksa
- dms-endpoint-ssl-configured
- dms-replication-not-public
- dms-replication-task-sourcedb-logging

- dms-replication-task-targetdb-logging
- docdb-cluster-encrypted-in-transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-optimized-instance
- ebs-snapshot-public-restorable-periksa
- ec2- ebs-encryption-by-default
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- 2-periksa launch-template-imdsv
- ec2- launch-template-public-ip -dinonaktifkan
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -periksa managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- paravirtual-instance-check

- ec2- -eni security-group-attached-to
- ec2-stopped-instance
- ec2- volume-inuse-check
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- terlampir eip
- eks-cluster-log-enabled
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan

- elasticache-repl-grp-encrypted-saat istirahat
- elasticache-repl-grp-encrypted-dalam transit
- elasticache-repl-grp-redis-auth-diaktifkan
- elasticache-subnet-group-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-managed-updates-diaktifkan
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -periksa predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-kerberos-enabled
- emr-master-no-public-ip
- volume terenkripsi
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-deployment-type-periksa
- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat

- glue-spark-job-supported-versi
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-customer-policy-blocked-kms-tindakan
- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa
- iam-root-access-key-periksa
- iam-user-group-membership-periksa
- iam-user-mfa-enabled
- iam-user-no-policies-periksa
- iam-user-unused-credentials-periksa
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check

- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- mfa-enabled-for-iam-akses konsol
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade diaktifkan
- mq-rabbit-deployment-mode
- msk-cluster-public-access-dinonaktifkan
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-update-check
- rabbit-mq-supported-version
- rds-automatic-minor-version-upgrade diaktifkan
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit

- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-diaktifkan
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-serverless-default-admin-periksa
- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi
- redshift-serverless-publish-logske cloudwatch
- tag yang dibutuhkan
- restricted-incoming-traffic
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication

- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- lifecycle-policy-check
- s3- version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-instance-root-akses-cek
- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub-enabled
- security-account-information-provided

- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notifikasi-diaktifkan
- sns-topic-no-public-akses
- sqs-queue-no-public-akses
- ssm-automation-block-public-berbagi
- ssm-automation-logging-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-diaktifkan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-connector-logging-enabled
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-sg-open-only-to-authorized-ports
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled
- wafv2- webacl-not-empty
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong

Wilayah Tiongkok (Ningxia)

Tiongkok (Ningxia)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- active-mq-supported-version

- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pengalihan-periksa
- alb-waf-enabled
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-istirahat
- athena-workgroup-logging-enabled
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- beanstalk-enhanced-health-reporting-diaktifkan
- clb-desync-mode-check

- clb-multiple-az
- cloudformation-stack-drift-detection-periksa
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-environment-privileged-periksa
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-periksa
- datasync-task-logging-enabled
- dax-encryption-enabled

- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-tingkatkan periksa
- dms-endpoint-ssl-configured
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-diaktifkan
- docdb-cluster-backup-retention-periksa
- docdb-cluster-deletion-protection-diaktifkan
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-optimized-instance
- ebs-snapshot-public-restorable-periksa
- ec2- ebs-encryption-by-default
- ec2- diaktifkan enis-source-destination-check
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check

- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- 2-periksa launch-template-imdsv
- ec2- launch-template-public-ip -dinonaktifkan
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -periksa managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- -eni security-group-attached-to
- ec2- - spot-fleet-request-ct encryption-at-rest
- ec2-stopped-instance
- ec2- volume-inuse-check
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted

- efs-in-backup-plan
- terlampir eip
- eks-cluster-log-enabled
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan
- elasticache-repl-grp-encrypted-saat istirahat
- elasticache-repl-grp-encrypted-dalam transit
- elasticache-repl-grp-redis-auth-diaktifkan
- elasticache-subnet-group-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-managed-updates-diaktifkan
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-kerberos-enabled

- emr-master-no-public-ip
- volume terenkripsi
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-deployment-type-periksa
- glue-job-logging-enabled
- glue-spark-job-supported-versi
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-customer-policy-blocked-kms-tindakan
- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa
- iam-root-access-key-periksa
- iam-user-group-membership-periksa
- iam-user-mfa-enabled
- iam-user-no-policies-periksa
- iam-user-unused-credentials-periksa
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- kinesis-stream-backup-retention-periksa

- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- mfa-enabled-for-iam-akses konsol
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade diaktifkan
- mq-rabbit-deployment-mode
- msk-cluster-public-access-dinonaktifkan
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-periksa
- neptune-cluster-cloudwatch-log-ekspor diaktifkan
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-diaktifkan
- neptune-cluster-encrypted
- neptune-cluster-iam-database-otentikasi
- neptune-cluster-multi-az-diaktifkan
- neptune-cluster-snapshot-encrypted
- no-unrestricted-route-to-igw
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-aurora-postgresql-logske cloudwatch
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-deletion-protection-diaktifkan

- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-diaktifkan
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan

- redshift-require-tls-ssl
- redshift-serverless-default-admin-periksa
- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi
- redshift-serverless-publish-logske cloudwatch
- tag yang dibutuhkan
- restricted-incoming-traffic
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- lifecycle-policy-check

- s3- version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-instance-root-akses-cek
- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notifikasi-diaktifkan
- sns-topic-no-public-akses
- sqs-queue-no-public-akses
- ssm-automation-block-public-berbagi
- ssm-automation-logging-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-diaktifkan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-connector-logging-enabled
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa

- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled
- wafv2- webacl-not-empty
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong
- workspaces-root-volume-encryption-diaktifkan
- workspaces-user-volume-encryption-diaktifkan

Wilayah Eropa (Frankfurt)

Eropa (Frankfurt)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pengalihan-periksa
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-penghapusan-diaktifkan
- amplify-app-description
- amplify-app-tagged

- amplify-branch-performance-mode-diaktifkan
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-tidak-kosong
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-penyimpanan
- appconfig-hosted-configuration-version-deskripsi
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-penerusan
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-default-tls

- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-akses
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-saat istirahat
- appsync-cache-ct-encryption-dalam transit
- appsync-cache-encryption-at-istirahat
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-istirahat
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat

- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-pencatatan
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapus-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-diaktifkan
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az

- cloudformation-stack-drift-detection-periksa
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-periksa
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- codedeploy-auto-rollback-monitor-diaktifkan
- codedeploy-deployment-group-auto-rollback-diaktifkan
- codedeploy-deployment-group-outdated-instances-pembaruan
- codedeploy-ec2- minimum-healthy-hosts-configured

- codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-akses-cek
- cognito-user-pool-advanced-keamanan diaktifkan
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-pembuatan profil
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-Terlampir
- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-tingkatkan periksa
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-diaktifkan
- dms-neptune-iam-authorization-diaktifkan
- dms-redis-tls-enabled
- dms-replication-not-public

- dms-replication-task-sourcedb-pencatatan
- dms-replication-task-tagged
- dms-replication-task-targetdb-pencatatan
- docdb-cluster-audit-logging-diaktifkan
- docdb-cluster-backup-retention-periksa
- docdb-cluster-deletion-protection-diaktifkan
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-dilarang
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- diaktifkan client-vpn-connection-log

- ec2- client-vpn-endpoint-tagged
- ec2- -semua client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- diaktifkan enis-source-destination-check
- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -dibuat last-backup-recovery-point
- ec2- 2-periksa launch-template-imdsv
- ec2- launch-template-public-ip -dinonaktifkan
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -periksa managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- network-insights-access-scope -analisis ditandai
- ec2- -ditandai network-insights-access-scope
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check

- ec2- prefix-list-tagged
- ec2- resources-in-logically-air -gapped-lemari besi
- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2- security-group-attached-to -eni-periodik
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan
- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi

- ecs-task-definition-memory-batas-keras
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-pengguna
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan
- terlampir eip
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versi
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan

- elasticache-repl-grp-encrypted-saat istirahat
- elasticache-repl-grp-encrypted-dalam transit
- elasticache-repl-grp-redis-auth-diaktifkan
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-logs-to-jam tangan awan
- elastic-beanstalk-managed-updates-diaktifkan
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -periksa predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-istirahat

- emr-security-configuration-encryption-transit
- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-konfigurasi-ada
- fis-experiment-template-tagged
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- fsx-last-backup-recovery-point-dibuat
- fsx-lustre-copy-tagsuntuk cadangan
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-audit-log-dikonfigurasi
- fsx-windows-deployment-type-periksa
- glb-listener-tagged
- global-endpoint-event-replication-diaktifkan
- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled

- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-tindakan
- iam-external-access-analyzer-diaktifkan
- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa
- iam-root-access-key-periksa
- iam-user-group-membership-periksa
- iam-user-mfa-enabled
- iam-user-no-policies-periksa
- iam-user-unused-credentials-periksa
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled

- inspector-lambda-code-scan-diaktifkan
- inspector-lambda-standard-scan-diaktifkan
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-diaktifkan
- ivs-channel-playback-authorization-diaktifkan
- ivs-channel-tagged
- ivs-playback-key-pair-ditandai
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan

- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-penemuan-cek
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-log
- mfa-enabled-for-iam-akses konsol
- mq-active-broker-ldap-otentikasi
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade diaktifkan
- mq-auto-minor-version-upgrade diaktifkan
- mq-broker-general-logging-diaktifkan
- mq-cloudwatch-audit-logging-diaktifkan
- mq-cloudwatch-audit-log-diaktifkan
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-dinonaktifkan
- msk-connect-connector-logging-diaktifkan
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls

- msk-unrestricted-access-check
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-periksa
- neptune-cluster-cloudwatch-log-ekspor diaktifkan
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-diaktifkan
- neptune-cluster-encrypted
- neptune-cluster-iam-database-otentikasi
- neptune-cluster-multi-az-diaktifkan
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-dilarang
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-cross-zone-load-menyeimbangkan diaktifkan
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-toleransi
- opensearch-encrypted-at-rest

- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-pemeriksaan enkripsi-
- opensearch-primary-node-fault-toleransi
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-aurora-postgresql-logske cloudwatch
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit

- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-diaktifkan
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-serverless-default-admin-periksa
- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi
- redshift-serverless-publish-logske cloudwatch
- redshift-serverless-workgroup-encrypted-dalam transit
- redshift-serverless-workgroup-no-akses publik
- redshift-serverless-workgroup-routes-dalam-vpc

- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-ember dengan tag
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check

- s3- meets-restore-time-target
- s3- resources-in-logically-air -gapped-lemari besi
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-ditandai
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-instance-root-akses-cek
- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub diaktifkan
- security-account-information-provided
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- sns-encrypted-kms

- sns-topic-message-delivery-notifikasi-diaktifkan
- sns-topic-no-public-akses
- sqs-queue-no-public-akses
- ssm-automation-block-public-berbagi
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-dibuat
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-rencana cadangan
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa

- vpc-peering-dns-resolution-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-kosong
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong
- workspaces-root-volume-encryption-diaktifkan
- workspaces-user-volume-encryption-diaktifkan

Wilayah Eropa (Irlandia)

Eropa (Irlandia)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pengalihan-periksa
- alb-internal-scheme-check
- alb-listener-tagged

- alb-waf-enabled
- amplify-app-branch-auto-penghapusan-diaktifkan
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-diaktifkan
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-tidak-kosong
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-penyimpanan
- appconfig-hosted-configuration-version-deskripsi
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-penerusan
- appmesh-mesh-tagged

- appmesh-route-tagged
- appmesh-virtual-gateway-backend-default-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-akses
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-istirahat
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-istirahat
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat

- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapus-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-diaktifkan
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az

- cloudformation-stack-drift-detection-periksa
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-periksa
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- codedeploy-auto-rollback-monitor-diaktifkan
- codedeploy-deployment-group-auto-rollback-diaktifkan
- codedeploy-deployment-group-outdated-instances-pembaruan
- codedeploy-ec2- minimum-healthy-hosts-configured

- codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-akses-cek
- cognito-user-pool-advanced-keamanan diaktifkan
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-Terlampir
- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-tingkatkan periksa
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-diaktifkan
- dms-neptune-iam-authorization-diaktifkan
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging

- docdb-cluster-audit-logging-diaktifkan
- docdb-cluster-backup-retention-periksa
- docdb-cluster-deletion-protection-diaktifkan
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-dilarang
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- diaktifkan client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -semua client-vpn-not-authorize
- ec2- dhcp-options-tagged

- ec2- ebs-encryption-by-default
- ec2- diaktifkan enis-source-destination-check
- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -dibuat last-backup-recovery-point
- ec2- 2-periksa launch-template-imdsv
- ec2- launch-template-public-ip -dinonaktifkan
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -periksa managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- network-insights-access-scope -analisis ditandai
- ec2- -ditandai network-insights-access-scope
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2- resources-in-logically-air -gapped-lemari besi
- ec2- -rencana resources-protected-by-backup

- ec2- -eni security-group-attached-to
- ec2- security-group-attached-to -eni-periodik
- ec2- - spot-fleet-request-ct encryption-at-rest
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan
- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi
- ecs-task-definition-memory-batas-keras
- ecs-task-definition-network-mode-not-host

- ecs-task-definition-nonroot-pengguna
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan
- terlampir eip
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versi
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan
- elasticache-repl-grp-encrypted-saat istirahat
- elasticache-repl-grp-encrypted-dalam transit

- elasticache-repl-grp-redis-auth-diaktifkan
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-logs-to-jam tangan awan
- elastic-beanstalk-managed-updates-diaktifkan
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -periksa predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-istirahat
- emr-security-configuration-encryption-transit
- volume terenkripsi

- event-data-store-cmk-enkripsi diaktifkan
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-konfigurasi-ada
- fis-experiment-template-tagged
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-dibuat
- fsx-lustre-copy-tagsuntuk cadangan
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-audit-log-dikonfigurasi
- fsx-windows-deployment-type-periksa
- glb-listener-tagged
- global-endpoint-event-replication-diaktifkan
- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat

- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-tindakan
- iam-external-access-analyzer-diaktifkan
- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa
- iam-root-access-key-periksa
- iam-user-group-membership-periksa
- iam-user-mfa-enabled
- iam-user-no-policies-periksa
- iam-user-unused-credentials-periksa
- incoming-ssh-disabled

- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-diaktifkan
- inspector-lambda-standard-scan-diaktifkan
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-diaktifkan
- ivs-channel-playback-authorization-diaktifkan
- ivs-channel-tagged
- ivs-playback-key-pair-ditandai
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa

- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-penemuan-cek
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-log
- mfa-enabled-for-iam-akses konsol
- mq-active-broker-ldap-otentikasi
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade diaktifkan
- mq-auto-minor-version-upgrade diaktifkan
- mq-broker-general-logging-diaktifkan
- mq-cloudwatch-audit-logging-diaktifkan
- mq-cloudwatch-audit-log-diaktifkan
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-dinonaktifkan
- msk-connect-connector-logging-diaktifkan

- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-periksa
- neptune-cluster-cloudwatch-log-ekspor diaktifkan
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-diaktifkan
- neptune-cluster-encrypted
- neptune-cluster-iam-database-otentikasi
- neptune-cluster-multi-az-diaktifkan
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-dilarang
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-cross-zone-load-menyeimbangkan diaktifkan
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled

- opensearch-data-node-fault-toleransi
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-pemeriksaan enkripsi-
- opensearch-primary-node-fault-toleransi
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-aurora-postgresql-logske cloudwatch
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-db-security-group-tidak diizinkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit

- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-diaktifkan
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-serverless-default-admin-periksa
- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi
- redshift-serverless-publish-logske cloudwatch

- redshift-serverless-workgroup-encrypted-dalam transit
- redshift-serverless-workgroup-no-akses publik
- redshift-serverless-workgroup-routes-dalam-vpc
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- s3 -aturan-periksa express-dir-bucket-lifecycle
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-ember dengan tag
- s3- bucket-versioning-enabled

- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -gapped-lemari besi
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-ditandai
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-instance-root-akses-cek
- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub diaktifkan

- security-account-information-provided
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notifikasi-diaktifkan
- sns-topic-no-public-akses
- sqs-queue-no-public-akses
- ssm-automation-block-public-berbagi
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-dibuat
- virtualmachine-resources-in-logically-air-gapped-vault

- virtualmachine-resources-protected-by-rencana cadangan
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-peering-dns-resolution-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-kosong
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong
- workspaces-root-volume-encryption-diaktifkan
- workspaces-user-volume-encryption-diaktifkan

Wilayah Eropa (London)

Eropa (London)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan
- active-mq-supported-version

- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pengalihan-periksa
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-penghapusan-diaktifkan
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-diaktifkan
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-tidak-kosong
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-penyimpanan

- appconfig-hosted-configuration-version-deskripsi
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-penerusan
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-default-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-akses
- apprunner-service-observability-enabled
- apprunner-service-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-istirahat
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description

- athena-workgroup-description
- athena-workgroup-encrypted-at-istirahat
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapus-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template

- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-diaktifkan
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-periksa
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-periksa
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi

- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- codedeploy-auto-rollback-monitor-diaktifkan
- codedeploy-deployment-group-auto-rollback-diaktifkan
- codedeploy-deployment-group-outdated-instances-pembaruan
- codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-akses-cek
- cognito-user-pool-advanced-keamanan diaktifkan
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-pembuatan profil
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-Terlampir
- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-tingkatkan periksa

- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-diaktifkan
- dms-neptune-iam-authorization-diaktifkan
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-diaktifkan
- docdb-cluster-backup-retention-periksa
- docdb-cluster-deletion-protection-diaktifkan
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-dilarang
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target
- ebs-optimized-instance

- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- diaktifkan client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -semua client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- diaktifkan enis-source-destination-check
- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -dibuat last-backup-recovery-point
- ec2- 2-periksa launch-template-imdsv
- ec2- launch-template-public-ip -dinonaktifkan
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -periksa managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check

- ec2- meets-restore-time-target
- ec2- network-insights-access-scope -analisis ditandai
- ec2- -ditandai network-insights-access-scope
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- resources-in-logically-air -gapped-lemari besi
- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2- security-group-attached-to -eni-periodik
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan
- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged

- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi
- ecs-task-definition-memory-batas-keras
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-pengguna
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan
- terlampir eip
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versi
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted

- elasticache-automatic-backup-check-diaktifkan
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan
- elasticache-repl-grp-encrypted-saat istirahat
- elasticache-repl-grp-encrypted-dalam transit
- elasticache-repl-grp-redis-auth-diaktifkan
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-logs-to-jam tangan awan
- elastic-beanstalk-managed-updates-diaktifkan
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -periksa predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa

- elb-tls-https-listeners-hanya
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-istirahat
- emr-security-configuration-encryption-transit
- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan
- fis-experiment-template-log-konfigurasi-ada
- fis-experiment-template-tagged
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- fsx-last-backup-recovery-point-dibuat
- fsx-lustre-copy-tagsuntuk cadangan
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-audit-log-dikonfigurasi
- fsx-windows-deployment-type-periksa
- glb-listener-tagged
- global-endpoint-event-replication-diaktifkan
- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan

- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-tindakan
- iam-external-access-analyzer-diaktifkan
- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa
- iam-root-access-key-periksa
- iam-user-group-membership-periksa
- iam-user-mfa-enabled
- iam-user-no-policies-periksa
- iam-user-unused-credentials-periksa
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-diaktifkan

- inspector-lambda-standard-scan-diaktifkan
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iot-authorizer-token-signing-diaktifkan
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-penemuan-cek
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-log
- mfa-enabled-for-iam-akses konsol
- mq-active-broker-ldap-otentikasi
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs

- mq-automatic-minor-version-upgrade diaktifkan
- mq-auto-minor-version-upgrade diaktifkan
- mq-broker-general-logging-diaktifkan
- mq-cloudwatch-audit-logging-diaktifkan
- mq-cloudwatch-audit-log-diaktifkan
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-dinonaktifkan
- msk-connect-connector-logging-diaktifkan
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-periksa
- neptune-cluster-cloudwatch-log-ekspor diaktifkan
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-diaktifkan
- neptune-cluster-encrypted
- neptune-cluster-iam-database-otentikasi
- neptune-cluster-multi-az-diaktifkan
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-dilarang
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait

- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-cross-zone-load-menyeimbangkan diaktifkan
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-toleransi
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-pemeriksaan enkripsi-
- opensearch-primary-node-fault-toleransi
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-aurora-postgresql-logske cloudwatch
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa

- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-diaktifkan
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az

- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-serverless-default-admin-periksa
- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi
- redshift-serverless-publish-logske cloudwatch
- redshift-serverless-workgroup-encrypted-dalam transit
- redshift-serverless-workgroup-no-akses publik
- redshift-serverless-workgroup-routes-dalam-vpc
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif

- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-ember dengan tag
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -gapped-lemari besi
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-ditandai
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-instance-root-akses-cek

- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub diaktifkan
- security-account-information-provided
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notifikasi-diaktifkan
- sns-topic-no-public-akses
- sqs-queue-no-public-akses
- ssm-automation-block-public-berbagi
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged

- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-dibuat
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-rencana cadangan
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-peering-dns-resolution-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-kosong
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong
- workspaces-root-volume-encryption-diaktifkan
- workspaces-user-volume-encryption-diaktifkan

Wilayah Eropa (Milan)

Eropa (Milan)

- access-keys-rotated

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pengalihan-periksa
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-penghapusan-diaktifkan
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-diaktifkan
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged

- appconfig-configuration-profile-validators-tidak-kosong
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-penyimpanan
- appconfig-hosted-configuration-version-deskripsi
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-penerusan
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-default-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-istirahat
- appsync-logging-enabled
- athena-data-catalog-description
- athena-workgroup-description

- athena-workgroup-encrypted-at-istirahat
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapus-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged

- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-diaktifkan
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-periksa
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-periksa
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa

- codebuild-report-group-encrypted-saat istirahat
- codedeploy-auto-rollback-monitor-diaktifkan
- codedeploy-deployment-group-auto-rollback-diaktifkan
- codedeploy-deployment-group-outdated-instances-pembaruan
- codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan
- codepipeline-deployment-count-check
- cognito-identity-pool-unauth-akses-cek
- cognito-user-pool-advanced-keamanan diaktifkan
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-tingkatkan periksa
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-diaktifkan
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-diaktifkan
- docdb-cluster-backup-retention-periksa

- docdb-cluster-deletion-protection-diaktifkan
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-dilarang
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- diaktifkan client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -semua client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- diaktifkan enis-source-destination-check
- ec2-fleet-tag
- ec2-imdsv2-periksa

- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -dibuat last-backup-recovery-point
- ec2- 2-periksa launch-template-imdsv
- ec2- launch-template-public-ip -dinonaktifkan
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- network-insights-access-scope -analisis ditandai
- ec2- -ditandai network-insights-access-scope
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- resources-in-logically-air -gapped-lemari besi
- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2- security-group-attached-to -eni-periodik
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged

- ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan
- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi
- ecs-task-definition-memory-batas-keras
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-pengguna
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target

- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan
- terlampir eip
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versi
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan
- elasticache-repl-grp-encrypted-saat istirahat
- elasticache-repl-grp-encrypted-dalam transit
- elasticache-repl-grp-redis-auth-diaktifkan
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-logs-to-jam tangan awan

- elastic-beanstalk-managed-updates-diaktifkan
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -periksa predefined-security-policy-ssl
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-istirahat
- emr-security-configuration-encryption-transit
- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan
- fis-experiment-template-log-konfigurasi-ada
- fis-experiment-template-tagged
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- fsx-last-backup-recovery-point-dibuat
- fsx-lustre-copy-tagsuntuk cadangan
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa

- fsx-resources-protected-by-rencana cadangan
- fsx-windows-audit-log-dikonfigurasi
- fsx-windows-deployment-type-periksa
- glb-listener-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-tindakan
- iam-external-access-analyzer-diaktifkan
- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa

- iam-root-access-key-periksa
- iam-user-group-membership-periksa
- iam-user-mfa-enabled
- iam-user-no-policies-periksa
- iam-user-unused-credentials-periksa
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-diaktifkan
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- macie-auto-sensitive-data-penemuan-cek
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-log
- mfa-enabled-for-iam-akses konsol
- mq-active-broker-ldap-otentikasi
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs

- mq-automatic-minor-version-upgrade diaktifkan
- mq-auto-minor-version-upgrade diaktifkan
- mq-broker-general-logging-diaktifkan
- mq-cloudwatch-audit-logging-diaktifkan
- mq-cloudwatch-audit-log-diaktifkan
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-dinonaktifkan
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-cross-zone-load-menyeimbangkan diaktifkan
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-toleransi

- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-pemeriksaan enkripsi-
- opensearch-primary-node-fault-toleransi
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-aurora-postgresql-logske cloudwatch
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-meets-restore-time-target
- rds-multi-az-support

- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-diaktifkan
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access

- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-ember dengan tag
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-ditandai
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi

- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-instance-root-akses-cek
- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub diaktifkan
- security-account-information-provided
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notifikasi-diaktifkan
- sns-topic-no-public-akses
- sqs-queue-no-public-akses
- ssm-automation-block-public-berbagi
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan

- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-dibuat
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-rencana cadangan
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-peering-dns-resolution-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty

- waf-regional-rulegroup-not-kosong
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong

Wilayah Eropa (Paris)

Eropa (Paris)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pengalihan-periksa
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-penghapusan-diaktifkan
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-diaktifkan
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi

- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-tidak-kosong
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-penyimpanan
- appconfig-hosted-configuration-version-deskripsi
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-penerusan
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-default-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id

- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-akses
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-istirahat
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-istirahat
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template

- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapus-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-diaktifkan
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-periksa
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check

- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-periksa
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- codedeploy-auto-rollback-monitor-diaktifkan
- codedeploy-deployment-group-auto-rollback-diaktifkan
- codedeploy-deployment-group-outdated-instances-pembaruan
- codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-akses-cek
- cognito-user-pool-advanced-keamanan diaktifkan
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-Terlampir
- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled

- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-tingkatkan periksa
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-diaktifkan
- dms-neptune-iam-authorization-diaktifkan
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-pencatatan
- dms-replication-task-tagged
- dms-replication-task-targetdb-pencatatan
- docdb-cluster-audit-logging-diaktifkan
- docdb-cluster-backup-retention-periksa
- docdb-cluster-deletion-protection-diaktifkan
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-dilarang
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan

- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- diaktifkan client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -semua client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- diaktifkan enis-source-destination-check
- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -dibuat last-backup-recovery-point
- ec2- 2-periksa launch-template-imdsv
- ec2- launch-template-public-ip -dinonaktifkan

- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -periksa managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- network-insights-access-scope -analisis ditandai
- ec2- -ditandai network-insights-access-scope
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- resources-in-logically-air -gapped-lemari besi
- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2- security-group-attached-to -eni-periodik
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan
- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled

- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi
- ecs-task-definition-memory-batas-keras
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-pengguna
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan
- terlampir eip

- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versi
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan
- elasticache-repl-grp-encrypted-saat istirahat
- elasticache-repl-grp-encrypted-dalam transit
- elasticache-repl-grp-redis-auth-diaktifkan
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-logs-to-jam tangan awan
- elastic-beanstalk-managed-updates-diaktifkan
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az

- elbv2- -periksa predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-istirahat
- emr-security-configuration-encryption-transit
- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan
- fis-experiment-template-log-konfigurasi-ada
- fis-experiment-template-tagged
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- fsx-last-backup-recovery-point-dibuat
- fsx-lustre-copy-tagsuntuk cadangan
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-audit-log-dikonfigurasi
- glb-listener-tagged

- global-endpoint-event-replication-diaktifkan
- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-tindakan
- iam-external-access-analyzer-diaktifkan
- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa
- iam-root-access-key-periksa
- iam-user-group-membership-periksa
- iam-user-mfa-enabled

- iam-user-no-policies-periksa
- iam-user-unused-credentials-periksa
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-diaktifkan
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- iot-authorizer-token-signing-diaktifkan
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-penemuan-cek
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-log
- mfa-enabled-for-iam-akses konsol
- mq-active-broker-ldap-otentikasi

- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade diaktifkan
- mq-auto-minor-version-upgrade diaktifkan
- mq-broker-general-logging-diaktifkan
- mq-cloudwatch-audit-logging-diaktifkan
- mq-cloudwatch-audit-log-diaktifkan
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-dinonaktifkan
- msk-connect-connector-logging-diaktifkan
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-periksa
- neptune-cluster-cloudwatch-log-ekspor diaktifkan
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-diaktifkan
- neptune-cluster-encrypted
- neptune-cluster-iam-database-otentikasi
- neptune-cluster-multi-az-diaktifkan
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-dilarang
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket

- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-cross-zone-load-menyeimbangkan diaktifkan
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-toleransi
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-pemeriksaan enkripsi-
- opensearch-primary-node-fault-toleransi
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-aurora-postgresql-logske cloudwatch
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan

- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-diaktifkan
- redshift-cluster-parameter-group-ditandai

- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-serverless-default-admin-periksa
- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi
- redshift-serverless-publish-logske cloudwatch
- redshift-serverless-workgroup-encrypted-dalam transit
- redshift-serverless-workgroup-no-akses publik
- redshift-serverless-workgroup-routes-dalam-vpc
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled

- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-ember dengan tag
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -gapped-lemari besi
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-ditandai
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi

- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-instance-root-akses-cek
- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notifikasi-diaktifkan
- sns-topic-no-public-akses
- sqs-queue-no-public-akses
- ssm-automation-block-public-berbagi
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged

- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-dibuat
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-rencana cadangan
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-peering-dns-resolution-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-kosong
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong

Wilayah Eropa (Spanyol)

Eropa (Spanyol)

- account-part-of-organizations

- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan
- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pengalihan-periksa
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled

- aurora-last-backup-recovery-point-dibuat
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-pencatatan
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapus-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging

- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type

- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ec2- capacity-reservation-tagged
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -dibuat last-backup-recovery-point

- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- prefix-list-tagged
- ec2- resources-in-logically-air -gapped-lemari besi
- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2-stopped-instance
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan
- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi
- ecs-task-definition-network-mode-not-host

- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan
- terlampir eip
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan
- elasticache-repl-grp-encrypted-saat istirahat
- elasticache-repl-grp-encrypted-dalam transit
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-

- elbv2-multiple-az
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-istirahat
- emr-security-configuration-encryption-transit
- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan
- fis-experiment-template-log-konfigurasi-ada
- fis-experiment-template-tagged
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- fsx-last-backup-recovery-point-dibuat
- fsx-lustre-copy-tagsuntuk cadangan
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-audit-log-dikonfigurasi
- fsx-windows-deployment-type-periksa
- glue-job-logging-enabled

- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-diaktifkan
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- mariadb-publish-logs-to-cloudwatch-log

- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan

- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-serverless-default-admin-periksa
- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi
- redshift-serverless-publish-logske cloudwatch
- redshift-serverless-workgroup-encrypted-dalam transit

- redshift-serverless-workgroup-no-akses publik
- redshift-serverless-workgroup-routes-dalam-vpc
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- bucket-ssl-requests-only
- s3-ember dengan tag
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check

- s3- meets-restore-time-target
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-ditandai
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-akses
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan

- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong

Wilayah Eropa (Stockholm)

Eropa (Stockholm)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan

- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pengalihan-periksa
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-penghapusan-diaktifkan
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-diaktifkan
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-tidak-kosong
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged

- appconfig-freeform-profile-config-penyimpanan
- appconfig-hosted-configuration-version-deskripsi
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-penerusan
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-default-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-istirahat
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-istirahat
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat
- aurora-meets-restore-time-target

- aurora-mysql-cluster-audit-pencatatan
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapus-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-diaktifkan
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-periksa
- cloudformation-stack-notification-check

- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-periksa
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- codedeploy-auto-rollback-monitor-diaktifkan
- codedeploy-deployment-group-auto-rollback-diaktifkan
- codedeploy-deployment-group-outdated-instances-pembaruan
- codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan
- codeguruprofiler-profiling-group-tagged

- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- cognito-identity-pool-unauth-akses-cek
- cognito-user-pool-advanced-keamanan diaktifkan
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-Terlampir
- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-tingkatkan periksa
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-diaktifkan
- dms-neptune-iam-authorization-diaktifkan
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-pencatatan
- dms-replication-task-tagged
- dms-replication-task-targetdb-pencatatan
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target

- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- diaktifkan client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -semua client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- diaktifkan enis-source-destination-check
- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -dibuat last-backup-recovery-point
- ec2- 2-periksa launch-template-imdsv

- ec2- launch-template-public-ip -dinonaktifkan
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -periksa managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- network-insights-access-scope -analisis ditandai
- ec2- -ditandai network-insights-access-scope
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- resources-in-logically-air -gapped-lemari besi
- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2- security-group-attached-to -eni-periodik
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan
- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check

- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi
- ecs-task-definition-memory-batas-keras
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-pengguna
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan

- terlampir eip
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versi
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan
- elasticache-repl-grp-encrypted-saat istirahat
- elasticache-repl-grp-encrypted-dalam transit
- elasticache-repl-grp-redis-auth-diaktifkan
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-logs-to-jam tangan awan
- elastic-beanstalk-managed-updates-diaktifkan
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit

- elbv2-multiple-az
- elbv2- -periksa predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-istirahat
- emr-security-configuration-encryption-transit
- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-konfigurasi-ada
- fis-experiment-template-tagged
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- fsx-last-backup-recovery-point-dibuat
- fsx-lustre-copy-tagsuntuk cadangan

- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-audit-log-dikonfigurasi
- fsx-windows-deployment-type-periksa
- glb-listener-tagged
- global-endpoint-event-replication-diaktifkan
- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-tindakan
- iam-external-access-analyzer-diaktifkan
- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa
- iam-password-policy

- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa
- iam-root-access-key-periksa
- iam-user-group-membership-periksa
- iam-user-mfa-enabled
- iam-user-no-policies-periksa
- iam-user-unused-credentials-periksa
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-diaktifkan
- inspector-lambda-standard-scan-diaktifkan
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- iot-authorizer-token-signing-diaktifkan
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc

- lambda-vpc-multi-az-periksa
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-penemuan-cek
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-log
- mfa-enabled-for-iam-akses konsol
- mq-active-broker-ldap-otentikasi
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade diaktifkan
- mq-auto-minor-version-upgrade diaktifkan
- mq-broker-general-logging-diaktifkan
- mq-cloudwatch-audit-logging-diaktifkan
- mq-cloudwatch-audit-log-diaktifkan
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-dinonaktifkan
- msk-connect-connector-logging-diaktifkan
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-periksa
- neptune-cluster-cloudwatch-log-ekspor diaktifkan
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-diaktifkan

- neptune-cluster-encrypted
- neptune-cluster-iam-database-otentikasi
- neptune-cluster-multi-az-diaktifkan
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-dilarang
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-cross-zone-load-menyeimbangkan diaktifkan
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-toleransi
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-pemeriksaan enkripsi-
- opensearch-primary-node-fault-toleransi
- opensearch-update-check
- rabbit-mq-supported-version

- rds-aurora-mysql-audit-logging-diaktifkan
- rds-aurora-postgresql-logske cloudwatch
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit

- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-diaktifkan
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-serverless-default-admin-periksa
- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi
- redshift-serverless-publish-logske cloudwatch
- redshift-serverless-workgroup-encrypted-dalam transit
- redshift-serverless-workgroup-no-akses publik
- redshift-serverless-workgroup-routes-dalam-vpc
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- s3 -aturan-periksa express-dir-bucket-lifecycle
- s3- -hanya access-point-in-vpc

- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-ember dengan tag
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -gapped-lemari besi
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-ditandai
- sagemaker-domain-in-vpc

- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-instance-root-akses-cek
- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notifikasi-diaktifkan
- sns-topic-no-public-akses
- sqs-queue-no-public-akses
- ssm-automation-block-public-berbagi
- ssm-automation-logging-enabled
- ssm-document-not-public

- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-dibuat
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-rencana cadangan
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-peering-dns-resolution-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled

- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-kosong
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong

Wilayah Eropa (Zürich)

Eropa (Zürich)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan
- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pengalihan-periksa
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-extension-association-tagged
- approved-amis-by-id

- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapusan-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged

- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- cognito-user-pool-tagged
- custom-eventbus-policy-attached

- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- diaktifkan client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- dhcp-options-tagged

- ec2- ebs-encryption-by-default
- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -dibuat last-backup-recovery-point
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- prefix-list-tagged
- ec2- resources-in-logically-air -gapped-lemari besi
- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2- - spot-fleet-request-ct encryption-at-rest
- ec2-stopped-instance
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan

- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan
- terlampir eip

- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan
- elasticache-repl-grp-encrypted-saat istirahat
- elasticache-repl-grp-encrypted-dalam transit
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elbv2-multiple-az
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-istirahat
- emr-security-configuration-encryption-transit
- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan

- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- fsx-last-backup-recovery-point-dibuat
- fsx-lustre-copy-tagsuntuk cadangan
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-audit-log-dikonfigurasi
- fsx-windows-deployment-type-periksa
- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-diaktifkan
- iam-password-policy
- incoming-ssh-disabled

- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-diaktifkan
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- mariadb-publish-logs-to-cloudwatch-log
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan

- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-aurora-postgresql-logske cloudwatch
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-snapshot-encrypted

- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-serverless-default-admin-periksa
- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi
- redshift-serverless-publish-logske cloudwatch
- redshift-serverless-workgroup-encrypted-dalam transit
- redshift-serverless-workgroup-no-akses publik
- redshift-serverless-workgroup-routes-dalam-vpc
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access

- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-ember dengan tag
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-no-direct-akses internet

- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-akses
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa

- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong

Wilayah Israel (Tel Aviv)

Israel (Tel Aviv)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan
- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pengalihan-periksa
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged

- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-tidak-kosong
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-penyimpanan
- appconfig-hosted-configuration-version-deskripsi
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-penerusan
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-default-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled

- aurora-mysql-cluster-audit-logging
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi

- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-user-pool-advanced-keamanan diaktifkan
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-optimized-instance
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2-imdsv2-periksa

- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- prefix-list-tagged
- ec2- -eni security-group-attached-to
- ec2-stopped-instance
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-periksa

- ecs-task-definition-user-for-host-mode-check
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-in-backup-plan
- efs-mount-target-public-dapat diakses
- terlampir eip
- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-periksa
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elbv2-multiple-az
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-block-public-access
- emr-kerberos-enabled
- emr-security-configuration-encryption-istirahat
- emr-security-configuration-encryption-transit
- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa

- fms-webacl-rulegroup-association-periksa
- fsx-lustre-copy-tagsuntuk cadangan
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa
- fsx-windows-deployment-type-periksa
- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- kinesis-firehose-delivery-stream-dienkripsi
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang

- lambda-function-settings-check
- lambda-inside-vpc
- macie-auto-sensitive-data-penemuan-cek
- mariadb-publish-logs-to-cloudwatch-log
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-periksa
- neptune-cluster-cloudwatch-log-ekspor diaktifkan
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-diaktifkan
- neptune-cluster-encrypted
- neptune-cluster-iam-database-otentikasi
- neptune-cluster-multi-az-diaktifkan
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat

- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-serverless-default-admin-periksa

- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi
- redshift-serverless-publish-logske cloudwatch
- redshift-serverless-workgroup-no-akses publik
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-ember dengan tag
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- lifecycle-policy-check

- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-ditandai
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-akses
- ssm-document-not-public
- ssm-document-tagged
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description

- transfer-workflow-tagged
- vpc-default-security-group-tertutup
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled
- wafv2- webacl-not-empty
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong

Wilayah Meksiko (Tengah)

Meksiko (Tengah)

- account-part-of-organizations
- acm-certificate-expiration-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pengalihan-periksa
- alb-waf-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launch-config-public-ip-dinonaktifkan
- cloudformation-stack-drift-detection-periksa
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check

- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- cw-loggroup-retention-period-periksa
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-public-restorable-periksa
- ec2- ebs-encryption-by-default
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached

- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- -eni security-group-attached-to
- ec2-stopped-instance
- ec2- volume-inuse-check
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan
- terlampir eip
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-periksa
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-kerberos-enabled
- emr-master-no-public-ip
- volume terenkripsi

- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- kms-cmk-not-scheduled-untuk-penghapusan
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-diaktifkan
- no-unrestricted-route-to-igw
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- tag yang dibutuhkan
- restricted-incoming-traffic
- s3- account-level-public-access -blok-periodik

- s3- bucket-blacklisted-actions-prohibited
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- secretsmanager-using-cmk
- Securityhub-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- subnet-auto-assign-public-ip-dinonaktifkan
- vpc-default-security-group-tertutup
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-terowongan

Wilayah Timur Tengah (Bahrain)

Timur Tengah (Bahrain)

- access-keys-rotated

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pengalihan-periksa
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-penghapusan-diaktifkan
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-diaktifkan
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged

- appconfig-configuration-profile-validators-tidak-kosong
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-penyimpanan
- appconfig-hosted-configuration-version-deskripsi
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-penerusan
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-default-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-saat istirahat
- appsync-cache-ct-encryption-dalam transit
- appsync-cache-encryption-at-istirahat
- appsync-logging-enabled
- athena-data-catalog-description

- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-istirahat
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat
- aurora-meets-restore-time-target
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapusan-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged

- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-diaktifkan
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-periksa
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-periksa
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa

- codebuild-report-group-encrypted-saat istirahat
- codedeploy-auto-rollback-monitor-diaktifkan
- codedeploy-deployment-group-auto-rollback-diaktifkan
- codedeploy-deployment-group-outdated-instances-pembaruan
- codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan
- cognito-identity-pool-unauth-akses-cek
- cognito-user-pool-advanced-keamanan diaktifkan
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-tingkatkan periksa
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-diaktifkan
- dms-neptune-iam-authorization-diaktifkan
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan

- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- diaktifkan client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -semua client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- diaktifkan enis-source-destination-check
- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached

- ec2- -dibuat last-backup-recovery-point
- ec2- 2-periksa launch-template-imdsv
- ec2- launch-template-public-ip -dinonaktifkan
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -periksa managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- network-insights-access-scope -analisis ditandai
- ec2- -ditandai network-insights-access-scope
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- resources-in-logically-air -gapped-lemari besi
- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2- security-group-attached-to -eni-periodik
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan

- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi
- ecs-task-definition-memory-batas-keras
- ecs-task-definition-nonroot-pengguna
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan

- terlampir eip
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-versi
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan
- elasticache-repl-grp-encrypted-saat istirahat
- elasticache-repl-grp-encrypted-dalam transit
- elasticache-repl-grp-redis-auth-diaktifkan
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-logs-to-jam tangan awan
- elastic-beanstalk-managed-updates-diaktifkan
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit

- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-istirahat
- emr-security-configuration-encryption-transit
- volume terenkripsi
- fis-experiment-template-log-konfigurasi-ada
- fis-experiment-template-tagged
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- fsx-last-backup-recovery-point-dibuat
- fsx-lustre-copy-tagsuntuk cadangan
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-diaktifkan
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-audit-log-dikonfigurasi
- glb-listener-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat
- guardduty-eks-protection-audit-diaktifkan

- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-tindakan
- iam-external-access-analyzer-diaktifkan
- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa
- iam-root-access-key-periksa
- iam-user-group-membership-periksa
- iam-user-mfa-enabled
- iam-user-no-policies-periksa
- iam-user-unused-credentials-periksa
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-diaktifkan
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya

- iot-authorizer-token-signing-diaktifkan
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- macie-auto-sensitive-data-penemuan-cek
- macie-status-check
- mfa-enabled-for-iam-akses konsol
- mq-active-broker-ldap-otentikasi
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade diaktifkan
- mq-auto-minor-version-upgrade diaktifkan
- mq-broker-general-logging-diaktifkan
- mq-cloudwatch-audit-logging-diaktifkan
- mq-cloudwatch-audit-log-diaktifkan
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-dinonaktifkan
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls

- msk-unrestricted-access-check
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-periksa
- neptune-cluster-cloudwatch-log-ekspor diaktifkan
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-diaktifkan
- neptune-cluster-encrypted
- neptune-cluster-iam-database-otentikasi
- neptune-cluster-multi-az-diaktifkan
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-dilarang
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- nlb-cross-zone-load-menyeimbangkan diaktifkan
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-toleransi
- opensearch-encrypted-at-rest
- opensearch-https-required

- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-pemeriksaan enkripsi-
- opensearch-primary-node-fault-toleransi
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-aurora-postgresql-logske cloudwatch
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-resources-protected-by-rencana cadangan

- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-diaktifkan
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication

- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-ember dengan tag
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -gapped-lemari besi
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-ditandai
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged

- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-root-akses-cek
- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notifikasi-diaktifkan
- sns-topic-no-public-akses
- ssm-automation-block-public-berbagi
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-agreement-description
- transfer-agreement-tagged

- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-dibuat
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-rencana cadangan
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-peering-dns-resolution-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-kosong
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong

Wilayah Timur Tengah (UEA)

Timur Tengah (UEA)

- account-part-of-organizations

- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pengalihan-periksa
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis

- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapusan-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging

- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- docdb-cluster-audit-logging-diaktifkan
- docdb-cluster-backup-retention-periksa

- docdb-cluster-deletion-protection-diaktifkan
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-dilarang
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-multiple-eni-check

- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -dibuat last-backup-recovery-point
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -periksa managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- prefix-list-tagged
- ec2- resources-in-logically-air -gapped-lemari besi
- ec2- -rencana resources-protected-by-backup
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan
- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets

- ecs-task-definition-log-konfigurasi
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-periksa
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan
- elasticache-redis-cluster-automatic-backup-periksa
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa

- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-istirahat
- emr-security-configuration-encryption-transit
- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- fsx-last-backup-recovery-point-dibuat
- fsx-lustre-copy-tagsuntuk cadangan
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-audit-log-dikonfigurasi
- fsx-windows-deployment-type-periksa
- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan

- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-diaktifkan
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- iot-authorizer-token-signing-diaktifkan
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- mariadb-publish-logs-to-cloudwatch-log
- mq-active-broker-ldap-otentikasi
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-upgrade diaktifkan

- mq-broker-general-logging-diaktifkan
- mq-cloudwatch-audit-log-diaktifkan
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-periksa
- neptune-cluster-cloudwatch-log-ekspor diaktifkan
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-diaktifkan
- neptune-cluster-encrypted
- neptune-cluster-iam-database-otentikasi
- neptune-cluster-multi-az-diaktifkan
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-dilarang
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh
- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-diaktifkan

- rds-aurora-postgresql-logske cloudwatch
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted

- redshift-backup-enabled
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-ditandai
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-serverless-default-admin-periksa
- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi
- redshift-serverless-publish-logske cloudwatch
- redshift-serverless-workgroup-no-akses publik
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled

- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-ember dengan tag
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-ditandai
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk

- Securityhub diaktifkan
- security-account-information-provided
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-akses
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa

- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong

Wilayah Amerika Selatan (Sao Paulo)

Amerika Selatan (Sao Paulo)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-dinonaktifkan
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-diaktifkan
- alb-http-to-https-pengalihan-periksa
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-penghapusan-diaktifkan
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-diaktifkan
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured

- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-tidak-kosong
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicateuntuk-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-penyimpanan
- appconfig-hosted-configuration-version-deskripsi
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-penerusan
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-default-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged

- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-saat istirahat
- appsync-cache-ct-encryption-dalam transit
- appsync-cache-encryption-at-istirahat
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-istirahat
- athena-workgroup-enforce-workgroup-konfigurasi
- athena-workgroup-engine-version-upgrade otomatis
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-rencana cadangan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-batas
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types

- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapusan-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-diaktifkan
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-periksa
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-periksa
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted

- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-periksa
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- codedeploy-auto-rollback-monitor-diaktifkan
- codedeploy-deployment-group-auto-rollback-diaktifkan
- codedeploy-deployment-group-outdated-instances-pembaruan
- codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-akses-cek
- cognito-user-pool-advanced-keamanan diaktifkan
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-Terlampir
- cw-loggroup-retention-period-periksa
- datasync-task-data-verification-diaktifkan
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled

- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-tingkatkan periksa
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-diaktifkan
- dms-neptune-iam-authorization-diaktifkan
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-diaktifkan
- docdb-cluster-backup-retention-periksa
- docdb-cluster-deletion-protection-diaktifkan
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-dilarang
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled

- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- capacity-reservation-tagged
- ec2- diaktifkan client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -semua client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- diaktifkan enis-source-destination-check
- ec2-fleet-tag
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- -dibuat last-backup-recovery-point
- ec2- 2-periksa launch-template-imdsv
- ec2- launch-template-public-ip -dinonaktifkan
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required

- ec2- -periksa managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- network-insights-access-scope -analisis ditandai
- ec2- -ditandai network-insights-access-scope
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2- resources-in-logically-air -gapped-lemari besi
- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2- security-group-attached-to -eni-periodik
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan
- ec2- -ditandai transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi

- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-no-environment-secrets
- ecs-task-definition-log-konfigurasi
- ecs-task-definition-memory-batas-keras
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-pengguna
- ecs-task-definition-pid-mode-periksa
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-direktori
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-meets-restore-time-target
- efs-mount-target-public-dapat diakses
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-rencana cadangan
- terlampir eip
- eks-cluster-logging-enabled
- eks-cluster-log-enabled

- eks-cluster-oldest-supported-versi
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan
- elasticache-auto-minor-version-tingkatkan periksa
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-periksa
- elasticache-repl-grp-auto-failover-diaktifkan
- elasticache-repl-grp-encrypted-saat istirahat
- elasticache-repl-grp-encrypted-dalam transit
- elasticache-repl-grp-redis-auth-diaktifkan
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-logs-to-jam tangan awan
- elastic-beanstalk-managed-updates-diaktifkan
- elbv2- acm-certificate-required
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -periksa predefined-security-policy-ssl
- elb-acm-certificate-required

- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-istirahat
- emr-security-configuration-encryption-transit
- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan
- fis-experiment-template-log-konfigurasi-ada
- fis-experiment-template-tagged
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- fsx-last-backup-recovery-point-dibuat
- fsx-lustre-copy-tagsuntuk cadangan
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-copy-tags-diaktifkan
- fsx-openzfs-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-audit-log-dikonfigurasi
- fsx-windows-deployment-type-periksa
- glb-listener-tagged
- global-endpoint-event-replication-diaktifkan

- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- penjaga-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-diaktifkan
- guardduty-eks-protection-audit-diaktifkan
- guardduty-eks-protection-runtime-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-tindakan
- iam-external-access-analyzer-diaktifkan
- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa
- iam-root-access-key-periksa
- iam-user-group-membership-periksa
- iam-user-mfa-enabled
- iam-user-no-policies-periksa

- iam-user-unused-credentials-periksa
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-diaktifkan
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-diaktifkan
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- kms-key-policy-no-akses publik
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-periksa
- macie-auto-sensitive-data-penemuan-cek
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-log
- mfa-enabled-for-iam-akses konsol
- mq-active-broker-ldap-otentikasi
- mq-active-deployment-mode

- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade diaktifkan
- mq-auto-minor-version-upgrade diaktifkan
- mq-broker-general-logging-diaktifkan
- mq-cloudwatch-audit-logging-diaktifkan
- mq-cloudwatch-audit-log-diaktifkan
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-dinonaktifkan
- msk-connect-connector-logging-diaktifkan
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-membutuhkan-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-periksa
- neptune-cluster-cloudwatch-log-ekspor diaktifkan
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-diaktifkan
- neptune-cluster-encrypted
- neptune-cluster-iam-database-otentikasi
- neptune-cluster-multi-az-diaktifkan
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-dilarang
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragmen-paket
- netfw-policy-default-action-paket penuh

- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-cross-zone-load-menyeimbangkan diaktifkan
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-toleransi
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-pemeriksaan enkripsi-
- opensearch-primary-node-fault-toleransi
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-diaktifkan
- rds-aurora-postgresql-logske cloudwatch
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-periksa
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-encrypted-at-istirahat
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-db-security-group-tidak diizinkan

- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-rencana cadangan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-diaktifkan
- redshift-cluster-parameter-group-ditandai

- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-periksa
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-serverless-default-admin-periksa
- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi
- redshift-serverless-publish-logske cloudwatch
- redshift-serverless-workgroup-no-akses publik
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- root-account-hardware-mfa-diaktifkan
- root-account-mfa-enabled
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif

- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3-ember dengan tag
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check
- s3- meets-restore-time-target
- s3- resources-in-logically-air -gapped-lemari besi
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-app-image-config-ditandai
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-instance-root-akses-cek

- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub diaktifkan
- security-account-information-provided
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notifikasi-diaktifkan
- sns-topic-no-public-akses
- sqs-queue-no-public-akses
- ssm-automation-block-public-berbagi
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-diaktifkan
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged

- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-dibuat
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-rencana cadangan
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-peering-dns-resolution-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan
- wafv2- rulegroup-logging-enabled
- wafv2- rulegroup-not-empty
- wafv2- webacl-not-empty
- waf-regional-rulegroup-not-kosong
- waf-regional-rule-not-kosong
- waf-regional-webacl-not-kosong
- workspaces-root-volume-encryption-diaktifkan
- workspaces-user-volume-encryption-diaktifkan

AWS GovCloud Wilayah (AS-Timur)

AWS GovCloud (AS-Timur)

- access-keys-rotated

- account-part-of-organizations
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-diaktifkan
- alb-http-to-https-pengalihan-periksa
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat
- aurora-mysql-cluster-audit-logging
- aurora-resources-protected-by-rencana cadangan
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapusan-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi
- beanstalk-enhanced-health-reporting-diaktifkan
- clb-desync-mode-check

- cloudformation-stack-drift-detection-periksa
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-environment-privileged-periksa
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- cw-loggroup-retention-period-periksa
- datasync-task-logging-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-mongo-db-authentication-diaktifkan

- dms-neptune-iam-authorization-diaktifkan
- dms-redis-tls-enabled
- dms-replication-not-public
- docdb-cluster-encrypted-in-transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-optimized-instance
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- diaktifkan client-vpn-connection-log
- ec2- ebs-encryption-by-default
- ec2- diaktifkan enis-source-destination-check
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- dibuat last-backup-recovery-point

- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -periksa managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2-stopped-instance
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan
- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-mount-target-public-dapat diakses
- efs-resources-protected-by-rencana cadangan

- terlampir eip
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan
- elasticache-redis-cluster-automatic-backup-periksa
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-managed-updates-diaktifkan
- elbv2- listener-encryption-in-transit
- elbv2- -periksa predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-kerberos-enabled
- emr-master-no-public-ip
- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- fsx-last-backup-recovery-point-dibuat

- fsx-ontap-deployment-type-periksa
- fsx-openzfs-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-deployment-type-periksa
- glue-job-logging-enabled
- glue-spark-job-supported-versi
- guardduty-eks-protection-audit-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-non-archived-findings
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-tindakan
- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa
- iam-root-access-key-periksa
- iam-user-group-membership-periksa
- iam-user-mfa-enabled
- iam-user-no-policies-periksa
- iam-user-unused-credentials-periksa
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled

- inspector-lambda-standard-scan-diaktifkan
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- mariadb-publish-logs-to-cloudwatch-log
- mfa-enabled-for-iam-akses konsol
- mq-cloudwatch-audit-log-diaktifkan
- msk-cluster-public-access-dinonaktifkan
- msk-unrestricted-access-check
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-primary-node-fault-toleransi
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-postgresql-logske cloudwatch

- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa
- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-resources-protected-by-rencana cadangan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-diaktifkan

- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-serverless-default-admin-periksa
- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi
- redshift-unrestricted-port-access
- tag yang dibutuhkan
- restricted-incoming-traffic
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only

- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi
- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub-enabled
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-automation-block-public-berbagi
- ssm-automation-logging-enabled
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-connector-logging-enabled
- transfer-family-server-no-ftp

- virtualmachine-last-backup-recovery-point-dibuat
- virtualmachine-resources-protected-by-rencana cadangan
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan

AWS GovCloud Wilayah (AS-Barat)

AWS GovCloud (AS-Barat)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-diaktifkan
- alb-http-to-https-pengalihan-periksa
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-dan-dienkripsi
- api-gw-endpoint-type-periksa
- api-gw-execution-logging-diaktifkan
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id

- approved-amis-by-tag
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-dibuat
- aurora-mysql-cluster-audit-logging
- aurora-resources-protected-by-rencana cadangan
- autoscaling-group-elb-healthcheck-diperlukan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-public-ip-dinonaktifkan
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-penghapusan-dinonaktifkan
- backup-recovery-point-minimum-pemeriksaan retensi
- beanstalk-enhanced-health-reporting-diaktifkan
- clb-desync-mode-check
- cloudformation-stack-drift-detection-periksa
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- cloudtrail-s3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-diaktifkan
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-diaktifkan
- cloud-trail-enabled

- cloud-trail-encryption-enabled
- cloud-trail-log-file-validasi-diaktifkan
- cmk-backing-key-rotation-diaktifkan
- codebuild-project-environment-privileged-periksa
- codebuild-project-envvar-awscred-periksa
- codebuild-project-logging-enabled
- codebuild-project-s3-log-terenkripsi
- codebuild-project-source-repo-url-periksa
- codebuild-report-group-encrypted-saat istirahat
- cognito-identity-pool-unauth-akses-cek
- connect-instance-logging-enabled
- cw-loggroup-retention-period-periksa
- datasync-task-logging-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-mongo-db-authentication-diaktifkan
- dms-neptune-iam-authorization-diaktifkan
- dms-redis-tls-enabled
- dms-replication-not-public
- docdb-cluster-encrypted-in-transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-dibuat
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-rencana cadangan
- dynamodb-table-deletion-protection-diaktifkan
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled

- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-dibuat
- ebs-optimized-instance
- ebs-resources-protected-by-rencana cadangan
- ebs-snapshot-public-restorable-periksa
- ec2- diaktifkan client-vpn-connection-log
- ec2- ebs-encryption-by-default
- ec2- diaktifkan enis-source-destination-check
- ec2-imdsv2-periksa
- ec2- instance-detailed-monitoring-enabled
- ec2- -ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- dibuat last-backup-recovery-point
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- -periksa managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- -periksa managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- -rencana resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2-stopped-instance
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-diaktifkan

- ecr-private-lifecycle-policy-dikonfigurasi
- ecr-private-tag-immutability-diaktifkan
- ecr-repository-cmk-encryption-diaktifkan
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-versi
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-identitas pengguna
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-dibuat
- efs-mount-target-public-dapat diakses
- efs-resources-protected-by-rencana cadangan
- terlampir eip
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-akses
- eks-secrets-encrypted
- elasticache-automatic-backup-check-diaktifkan
- elasticache-redis-cluster-automatic-backup-periksa
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-pemeriksaan enkripsi-
- elastic-beanstalk-managed-updates-diaktifkan

- elbv2- listener-encryption-in-transit
- elbv2- -periksa predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-menyeimbangkan diaktifkan
- elb-custom-security-policy-ssl-periksa
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-periksa
- elb-tls-https-listeners-hanya
- emr-kerberos-enabled
- emr-master-no-public-ip
- volume terenkripsi
- event-data-store-cmk-enkripsi diaktifkan
- fms-shield-resource-policy-periksa
- fms-webacl-resource-policy-periksa
- fms-webacl-rulegroup-association-periksa
- fsx-last-backup-recovery-point-dibuat
- fsx-ontap-deployment-type-periksa
- fsx-openzfs-deployment-type-periksa
- fsx-resources-protected-by-rencana cadangan
- fsx-windows-deployment-type-periksa
- glue-job-logging-enabled
- glue-ml-transform-encrypted-saat istirahat
- glue-spark-job-supported-versi
- guardduty-eks-protection-audit-diaktifkan
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-non-archived-findings
- guardduty-s3-protection-enabled

- iam-customer-policy-blocked-kms-tindakan
- iam-group-has-users-periksa
- iam-inline-policy-blocked-kms-tindakan
- iam-no-inline-policy-periksa
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-periksa
- iam-root-access-key-periksa
- iam-server-certificate-expiration-periksa
- iam-user-group-membership-periksa
- iam-user-mfa-enabled
- iam-user-no-policies-periksa
- iam-user-unused-credentials-periksa
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-diaktifkan
- instances-in-vpc
- internet-gateway-authorized-vpc-hanya
- kinesis-firehose-delivery-stream-dienkripsi
- kinesis-stream-backup-retention-periksa
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-untuk-penghapusan
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-dilarang

- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- mariadb-publish-logs-to-cloudwatch-log
- mfa-enabled-for-iam-akses konsol
- mq-cloudwatch-audit-log-diaktifkan
- msk-cluster-public-access-dinonaktifkan
- msk-unrestricted-access-check
- multi-region-cloud-trail-diaktifkan
- nacl-no-unrestricted-ssh-rdp
- netfw-policy-rule-group-terkait
- netfw-stateless-rule-group-tidak-kosong
- netfw-subnet-change-protection-diaktifkan
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-primary-node-fault-toleransi
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-postgresql-logske cloudwatch
- rds-automatic-minor-version-upgrade diaktifkan
- rds-cluster-deletion-protection-diaktifkan
- rds-cluster-iam-authentication-diaktifkan
- rds-cluster-multi-az-diaktifkan
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-periksa
- rds-instance-deletion-protection-diaktifkan
- rds-instance-iam-authentication-diaktifkan
- rds-instance-public-access-periksa
- rds-instance-subnet-igw-periksa

- rds-in-backup-plan
- rds-last-backup-recovery-point-dibuat
- rds-logging-enabled
- rds-mariadb-instance-encrypted-dalam transit
- rds-multi-az-support
- rds-mysql-instance-encrypted-dalam transit
- rds-postgresql-logs-to-jam tangan awan
- rds-postgres-instance-encrypted-dalam transit
- rds-resources-protected-by-rencana cadangan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logske cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-diaktifkan
- redshift-cluster-public-access-periksa
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-enhanced-vpc-routing-diaktifkan
- redshift-require-tls-ssl
- redshift-serverless-default-admin-periksa
- redshift-serverless-default-db-nama-cek
- redshift-serverless-namespace-cmk-enkripsi
- redshift-unrestricted-port-access
- tag yang dibutuhkan

- restricted-incoming-traffic
- s3- -hanya access-point-in-vpc
- s3- -blok access-point-public-access
- s3- -blok account-level-public-access
- s3- account-level-public-access -blok-periodik
- s3- bucket-acl-prohibited
- s3- bucket-blacklisted-actions-prohibited
- s3- -diaktifkan bucket-cross-region-replication
- s3- bucket-default-lock-enabled
- s3- -dilarang bucket-level-public-access
- s3- bucket-logging-enabled
- s3- bucket-mfa-delete-enabled
- s3- bucket-policy-grantee-check
- s3- bucket-policy-not-more -permisif
- s3- bucket-public-read-prohibited
- s3- bucket-public-write-prohibited
- s3- bucket-replication-enabled
- s3- -diaktifkan bucket-server-side-encryption
- s3- bucket-ssl-requests-only
- s3- bucket-versioning-enabled
- s3- default-encryption-kms
- s3- event-notifications-enabled
- s3- -dibuat last-backup-recovery-point
- s3- lifecycle-policy-check
- s3- -rencana resources-protected-by-backup
- s3- version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi
- sagemaker-endpoint-config-prod-hitungan contoh
- sagemaker-notebook-instance-kms-kunci-dikonfigurasi

- sagemaker-notebook-instance-platform-versi
- sagemaker-notebook-no-direct-akses internet
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-periksa
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- Securityhub diaktifkan
- service-catalog-shared-within-organisasi
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-automation-block-public-berbagi
- ssm-automation-logging-enabled
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-dibuat
- storagegateway-resources-protected-by-rencana cadangan
- subnet-auto-assign-public-ip-dinonaktifkan
- transfer-connector-logging-enabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-dibuat
- virtualmachine-resources-protected-by-rencana cadangan
- vpc-default-security-group-tertutup
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-periksa
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-periksa
- vpc-vpn-2-terowongan
- wafv2-logging-diaktifkan

- workspaces-root-volume-encryption-diaktifkan
- workspaces-user-volume-encryption-diaktifkan

Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template

> **Important**
>
> Anda harus terlebih dahulu membuat dan memulai perekam AWS Config konfigurasi untuk membuat aturan AWS Config terkelola dengan AWS CloudFormation. Untuk informasi selengkapnya, lihat Mengelola Perekam Konfigurasi.

Untuk aturan AWS Config terkelola yang didukung, Anda dapat menggunakan AWS CloudFormation templat untuk membuat aturan untuk akun Anda atau memperbarui AWS CloudFormation tumpukan yang ada. Tumpukan adalah kumpulan sumber daya terkait yang Anda sediakan dan perbarui sebagai satu unit. Saat Anda meluncurkan tumpukan dengan templat, aturan AWS Config terkelola dibuat untuk Anda. Template hanya membuat aturan, dan tidak membuat AWS sumber daya tambahan.

> **Note**
>
> Saat aturan AWS Config terkelola diperbarui, templat diperbarui untuk perubahan terbaru. Untuk menyimpan versi template tertentu sebagai aturan, unduh templat, dan unggah ke bucket S3 Anda.

Untuk informasi selengkapnya tentang bekerja dengan AWS CloudFormation templat, lihat Memulai AWS CloudFormation di Panduan AWS CloudFormation Pengguna.

Untuk meluncurkan AWS CloudFormation tumpukan untuk aturan AWS Config terkelola

1. Pergi ke CloudFormationkonsol dan buat tumpukan baru.
2. Untuk template Tentukan:
   - Jika Anda mengunduh templat, pilih Unggah file templat, lalu Pilih file untuk mengunggah templat.

- Anda juga dapat memilih URL Amazon S3, dan memasukkan URL template. `http://s3.amazonaws.com/aws-configservice-us-east-1/cloudformation-templates-for-managed-rules/THE_RULE_IDENTIFIER.template`

> **Note**
>
> Pengidentifikasi aturan harus ditulis dalam ALL_CAPS_WITH_UNDERSCORES. Misalnya, CLOUDWATCH_LOG_GROUP_ENCRYPTED, bukan. cloudwatch-log-group-encrypted
>
> Untuk beberapa aturan, pengidentifikasi aturan berbeda dari nama aturan. Pastikan untuk menggunakan pengenal aturan. Misalnya, pengidentifikasi aturan untuk restricted-ssh adalah INCOMING_SSH_DISABLED.

3. Pilih Berikutnya.
4. Untuk Tentukan detail tumpukan, ketik nama tumpukan dan masukkan nilai parameter untuk AWS Config aturan tersebut. Misalnya, jika Anda menggunakan templat aturan `DESIRED_INSTANCE_TYPE` terkelola, Anda dapat menentukan jenis instance seperti “m4.large”.
5. Pilih Berikutnya.
6. Untuk Opsi, Anda dapat membuat tag atau mengonfigurasi opsi lanjutan lainnya. Ini tidak diperlukan.
7. Pilih Berikutnya.
8. Untuk Tinjauan, verifikasi bahwa templat, parameter, dan opsi lainnya sudah benar.
9. Pilih Buat. Tumpukan dibuat dalam beberapa menit. Anda dapat melihat aturan yang dibuat di AWS Config konsol.

Anda dapat menggunakan template untuk membuat satu tumpukan untuk aturan AWS Config terkelola atau memperbarui tumpukan yang ada di akun Anda. Jika Anda menghapus tumpukan, aturan terkelola yang dibuat dari tumpukan itu juga akan dihapus. Untuk informasi selengkapnya, lihat Menggunakan Tumpukan dalam Panduan Pengguna AWS CloudFormation .

AWS Config Aturan Kustom

AWS Config Aturan Kustom adalah aturan yang Anda buat dari awal. Ada dua cara untuk membuat aturan AWS Config khusus: dengan fungsi Lambda (Panduan AWS Lambda Pengembang) dan dengan Guard (Guard GitHub Repository), sebuah bahasa. policy-as-code

AWS Config Aturan kustom yang dibuat dengan Lambda disebut Aturan AWS Config Lambda AWS Config Kustom dan aturan khusus yang dibuat dengan Guard disebut AWS Config Aturan Kebijakan Kustom.

Sebelum menggunakan aturan khusus, lihatPertimbangan.

AWS Config Aturan Kebijakan Kustom

Aturan yang ditulis menggunakan Guard dapat dibuat dari AWS Config konsol atau dengan menggunakan AWS Config aturan APIs. AWS Config Aturan Kebijakan Kustom memungkinkan Anda membuat aturan AWS Config Kustom tanpa perlu menggunakan Java atau Python untuk mengembangkan fungsi Lambda untuk mengelola aturan kustom Anda. AWS Config Aturan Kebijakan Kustom dimulai oleh perubahan konfigurasi. Untuk informasi lebih lanjut tentang Guard, lihat Guard GitHub Repository.

AWS Config Aturan Lambda Kustom

Aturan Lambda khusus memberi Anda opsi untuk menggunakan Java atau Python untuk membuat fungsi Lambda untuk aturan Kustom. AWS Config Fungsi Lambda adalah kode khusus yang Anda unggah AWS Lambda, dan dipanggil oleh peristiwa yang dipublikasikan oleh sumber peristiwa. Jika fungsi Lambda dikaitkan dengan AWS Config aturan, AWS Config memanggilnya saat aturan dimulai. Fungsi Lambda kemudian mengevaluasi informasi konfigurasi yang dikirim oleh AWS Config, dan mengembalikan hasil evaluasi. Untuk informasi selengkapnya tentang fungsi Lambda, lihat Sumber Fungsi dan Peristiwa di Panduan AWS Lambda Pengembang.

Perbedaan format untuk Aturan AWS Config Kustom

Tabel berikut menampilkan perbedaan format dalam bidang untuk tipe ConfigurationItemdata dan untuk Aturan AWS Config Kustom.

ConfigurationItem	AWS Config Aturan Kustom
`version`	`configurationItemVersion`
`accountId`	`awsAccountId`
`arn`	ARN
`configurationItemMD5Hash`	`configurationStateMd5Hash`

Topik

- Membuat Aturan Kebijakan AWS Config Kustom
- Membuat Aturan Lambda AWS Config Kustom
- Mengelola Sumber Daya yang Dihapus untuk AWS Config Aturan Lambda Kustom

Membuat Aturan Kebijakan AWS Config Kustom

Anda dapat membuat aturan Kebijakan AWS Config Kustom dari AWS Management Console, AWS CLI, atau AWS Config API.

Menambahkan aturan Kebijakan AWS Config Kustom

Using the console

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Di AWS Management Console menu, verifikasi bahwa pemilih Wilayah diatur ke AWS Wilayah yang mendukung AWS Config aturan. Untuk daftar Wilayah yang didukung, lihat AWS Config Wilayah dan Titik Akhir di. Referensi Umum Amazon Web Services
3. Di navigasi kiri, pilih Aturan.
4. Pada halaman Aturan, pilih Tambahkan aturan.
5. Pada halaman Tentukan tipe aturan, pilih Buat aturan kustom menggunakan Penjaga.
6. Pada halaman Konfigurasi aturan, buat aturan Anda dengan menyelesaikan langkah-langkah berikut:

    a. Untuk nama Aturan, ketikkan nama unik untuk aturan.

    b. Untuk Deskripsi, ketikkan deskripsi untuk aturan.

    c. Untuk versi runtime Guard, pilih sistem runtime untuk aturan Kebijakan AWS Config Kustom Anda.

    d. Untuk Konten Aturan, Anda dapat mengisinya dengan kebijakan Guard Custom untuk aturan Anda.

    e. Untuk mode Evaluasi, pilih kapan dalam proses pembuatan dan manajemen sumber daya Anda AWS Config ingin mengevaluasi sumber daya Anda. Tergantung pada aturan, AWS Config dapat mengevaluasi konfigurasi sumber daya Anda sebelum sumber daya telah disediakan, setelah sumber daya telah ditetapkan, atau keduanya.

i. Pilih Aktifkan evaluasi proaktif untuk memungkinkan Anda menjalankan evaluasi pada pengaturan konfigurasi sumber daya Anda sebelum diterapkan.

   Setelah mengaktifkan evaluasi proaktif, Anda dapat menggunakan StartResourceEvaluationAPI dan GetResourceEvaluationSummaryAPI untuk memeriksa apakah sumber daya yang Anda tentukan dalam perintah ini akan ditandai sebagai NON_COMPLIANT oleh aturan proaktif di akun Anda di Wilayah Anda.

   Untuk informasi selengkapnya tentang penggunaan perintah ini, lihat Mengevaluasi Sumber Daya Anda dengan AWS Config Aturan. Untuk daftar aturan terkelola yang mendukung evaluasi proaktif, lihat Daftar Aturan AWS Config Terkelola menurut Mode Evaluasi.

ii. Pilih Aktifkan evaluasi detektif untuk mengevaluasi pengaturan konfigurasi sumber daya yang ada.

   Untuk evaluasi detektif, aturan Kebijakan AWS Config Kustom dimulai oleh perubahan Konfigurasi. Opsi ini akan dipilih sebelumnya.

   - Sumber Daya — Saat sumber daya yang cocok dengan jenis sumber daya yang ditentukan, atau pengenal tipe plus, dibuat, diubah, atau dihapus.
   - Tag — Ketika sumber daya dengan tag yang ditentukan dibuat, diubah, atau dihapus.
   - Semua perubahan — Ketika sumber daya yang direkam oleh AWS Config dibuat, diubah, atau dihapus.

   AWS Config menjalankan evaluasi saat mendeteksi perubahan pada sumber daya yang cocok dengan cakupan aturan. Anda dapat menggunakan ruang lingkup untuk membatasi sumber daya mana yang memulai evaluasi. Jika tidak, evaluasi dimulai ketika ada perubahan pada sumber daya pasca-penyediaan.

f. Untuk Parameter, Anda dapat menyesuaikan nilai untuk kunci yang disediakan jika aturan Anda menyertakan parameter. Parameter adalah atribut yang harus dipatuhi oleh sumber daya Anda sebelum dianggap sesuai dengan aturan.

7. Pada halaman Tinjau dan buat, tinjau semua pilihan Anda sebelum menambahkan aturan ke halaman Anda Akun AWS.
8. Setelah selesai meninjau aturan, pilih Tambahkan aturan.

Using the AWS CLI

Gunakan perintah `put-config-rule`.

`Owner`Bidang harus`CUSTOM_POLICY`. Bidang tambahan berikut diperlukan untuk aturan Kebijakan AWS Config Kustom:

- `Runtime`: Sistem runtime untuk aturan Kebijakan AWS Config Kustom Anda.
- `PolicyText`: Definisi kebijakan yang berisi logika untuk aturan Kebijakan AWS Config Kustom Anda.
- `EnableDebugLogDelivery`: Ekspresi Boolean untuk mengaktifkan logging debug untuk aturan Kebijakan AWS Config Kustom Anda. Nilai default-nya adalah `false`.

Using the API Reference

Gunakan PutConfigRuletindakan.

`Owner`Bidang harus`CUSTOM_POLICY`. Bidang tambahan berikut diperlukan untuk aturan Kebijakan AWS Config Kustom:

- `Runtime`: Sistem runtime untuk aturan Kebijakan AWS Config Kustom Anda.
- `PolicyText`: Definisi kebijakan yang berisi logika untuk aturan Kebijakan AWS Config Kustom Anda.
- `EnableDebugLogDelivery`: Ekspresi Boolean untuk mengaktifkan logging debug untuk aturan Kebijakan AWS Config Kustom Anda. Nilai default-nya adalah `false`.

Menulis konten aturan untuk aturan Kebijakan AWS Config Kustom

Dengan aturan Kebijakan AWS Config Khusus, Anda dapat menggunakan bahasa khusus domain (DSL) AWS CloudFormation Guard untuk mengevaluasi konfigurasi sumber daya. Topik ini menyediakan pola dan praktik terbaik untuk menulis aturan kebijakan khusus.

Untuk informasi selengkapnya tentang cara menulis aturan dengan Guard, lihat Menulis aturan Guard di AWS CloudFormation Guard User Guide dan AWS CloudFormation Guard 2.0 Modes of Operation in the Guard GitHub Repository.

Struktur aturan dasar

Gunakan format dasar berikut untuk membuat aturan:

```
# Basic rule format
rule <rule_name> when
    resourceType == "<AWS::Service::Resource>" {
    # Evaluation clauses
}

# Example with filtering
let resources_of_type = Resources.*[ Type == 'AWS::Service::Resource' ]
rule check_resources when %resources_of_type !empty {
    %resources_of_type.configuration.property == expected_value
}
```

Komponen kunci

konfigurasi

Berisi isi untuk konfigurasi sumber daya.

SuplementaryConfiguration

Berisi konten tambahan untuk konfigurasi sumber daya. AWS Config mengembalikan bidang ini untuk jenis sumber daya tertentu untuk melengkapi informasi yang dikembalikan untuk bidang konfigurasi.

resourceType

AWS jenis sumber daya yang sedang dievaluasi.

resourceId

ID sumber daya (misalnya,`sg-xxxxxx`).

accountId

Akun AWS ID 12 digit yang terkait dengan sumber daya.

Pola umum

Status checks

```
let allowed_status = ['ACTIVE', 'RUNNING']
rule check_resource_status when
```

```
    resourceType == "AWS::Service::Resource" {
    configuration.status IN %allowed_status
}
```

Required properties

```
rule check_required_properties when
    resourceType == "AWS::Service::Resource" {
    configuration.propertyName exists
    configuration.propertyName is_string  # or is_list, is_struct
}
```

Query blocks

```
configuration.Properties {
    property1 exists
    property2 is_string
    property3 IN [allowed_value1, allowed_value2]
}
```

Conditional evaluation

```
when configuration.feature_enabled == true {
    configuration.feature_settings exists
    configuration.feature_settings is_struct
}
```

Custom messages

```
rule check_compliance when
    resourceType == "AWS::Service::Resource" {
    configuration.property == expected_value <<Custom error message explaining the
 requirement>>
}}
```

Fitur lanjutan

Range checks

```
rule check_numeric_limits {
```

```
    # Inclusive range (lower_limit <= value <= upper_limit)
    configuration.value IN r[minimum_value, maximum_value]

    # Exclusive range (lower_limit < value < upper_limit)
    configuration.value IN r(exclusive_min, exclusive_max)

    # Left inclusive, right exclusive (lower_limit <= value < upper_limit)
    configuration.value IN r[minimum_value, exclusive_max)

    # Left exclusive, right inclusive (lower_limit < value <= upper_limit)
    configuration.value IN r(exclusive_min, maximum_value]
}
```

Combining conditions

```
# AND conditions (implicit through new lines)
condition_1
condition_2

# OR conditions (explicit)
condition_3 OR
condition_4
```

Chaining rules

```
rule check_prerequisites {
    configuration.required_setting exists
}

rule check_details when check_prerequisites {
    configuration.required_setting == expected_value
}
```

Praktik terbaik

- Gunakan variabel dengan `let` pernyataan untuk meningkatkan keterbacaan.
- Pemeriksaan terkait grup menggunakan blok aturan bernama.
- Sertakan komentar deskriptif.
- Gunakan operator yang sesuai (`exists`,`is_string`,`is_list`).
- Gunakan pola regex dengan pencocokan case-insensitive.

Contoh: dynamodb-pitr-enabled

Contoh berikut menunjukkan definisi kebijakan untuk versi aturan Kebijakan AWS Config Kustom dari aturan AWS Config Terkeloladynamodb-pitr-enabled. Aturan ini memeriksa apakah tabel Point-in-Time DynamoDB telah mengaktifkan Pemulihan.

```
# Check if DynamoDB tables have Point-in-Time Recovery enabled
let status = ['ACTIVE']

rule tableisactive when
    resourceType == "AWS::DynamoDB::Table" {
    configuration.tableStatus == %status
}

rule checkcompliance when
    resourceType == "AWS::DynamoDB::Table"
    tableisactive {
    let pitr =
 supplementaryConfiguration.ContinuousBackupsDescription.pointInTimeRecoveryDescription.pointIn
    %pitr == "ENABLED" <<DynamoDB tables must have Point-in-Time Recovery enabled>>
}
```

Membuat Aturan Lambda AWS Config Kustom

Anda dapat mengembangkan aturan khusus dan menambahkannya AWS Config dengan AWS Lambda fungsi.

Anda mengaitkan setiap aturan kustom dengan fungsi Lambda, yang berisi logika yang mengevaluasi apakah AWS sumber daya Anda mematuhi aturan. Anda mengaitkan fungsi ini dengan aturan Anda, dan aturan memanggil fungsi baik sebagai respons terhadap perubahan konfigurasi atau secara berkala. Fungsi tersebut kemudian mengevaluasi apakah sumber daya Anda mematuhi aturan Anda, dan mengirimkan hasil evaluasinya ke AWS Config.

AWS Kit Pengembangan Aturan (RDK)

AWS Rule Development Kit (RDK) dirancang untuk mendukung alur kerja “Compliance-as-Code” yang intuitif dan produktif. Ini mengabstraksi sebagian besar angkat berat yang tidak berdiferensiasi yang terkait dengan penerapan AWS Config aturan yang didukung oleh fungsi Lambda khusus, dan menyediakan proses iteratif yang efisien. develop-deploy-monitor

Untuk step-by-step instruksi, lihat Dokumentasi AWS Rule Development Kit (RDK).

Contoh AWS Lambda Fungsi untuk AWS Config Aturan (Node.js)

AWS Lambda menjalankan fungsi dalam menanggapi peristiwa yang diterbitkan oleh AWS layanan. Fungsi untuk aturan Lambda AWS Config Kustom menerima peristiwa yang diterbitkan oleh AWS Config, dan fungsi tersebut kemudian menggunakan data yang diterimanya dari acara dan diambil dari AWS Config API untuk mengevaluasi kepatuhan aturan. Operasi dalam fungsi untuk aturan Config berbeda tergantung pada apakah ia melakukan evaluasi yang dipicu oleh perubahan konfigurasi atau dipicu secara berkala.

Untuk informasi tentang pola umum dalam AWS Lambda fungsi, lihat Model Pemrograman di Panduan AWS Lambda Pengembang.

Example Function for Evaluations Triggered by Configuration Changes

AWS Config akan memanggil fungsi seperti contoh berikut ketika mendeteksi perubahan konfigurasi untuk sumber daya yang berada dalam cakupan aturan khusus.

Jika Anda menggunakan AWS Config konsol untuk membuat aturan yang terkait dengan fungsi seperti contoh ini, pilih Perubahan konfigurasi sebagai jenis pemicu. Jika Anda menggunakan AWS Config API atau AWS CLI untuk membuat aturan, atur `MessageType` atribut ke `ConfigurationItemChangeNotification` dan`OversizedConfigurationItemChangeNotification`. Pengaturan ini memungkinkan aturan Anda dipicu setiap kali AWS Config menghasilkan item konfigurasi atau item konfigurasi yang terlalu besar sebagai akibat dari perubahan sumber daya.

Contoh ini mengevaluasi sumber daya Anda dan memeriksa apakah instance cocok dengan jenis sumber daya. `AWS::EC2::Instance` Aturan dipicu saat AWS Config menghasilkan item konfigurasi atau pemberitahuan item konfigurasi berukuran besar.

```
'use strict';

import { ConfigServiceClient, GetResourceConfigHistoryCommand,
 PutEvaluationsCommand } from "@aws-sdk/client-config-service";

const configClient = new ConfigServiceClient({});

// Helper function used to validate input
function checkDefined(reference, referenceName) {
    if (!reference) {
        throw new Error(`Error: ${referenceName} is not defined`);
    }
```

```
    return reference;
}

// Check whether the message type is OversizedConfigurationItemChangeNotification,
function isOverSizedChangeNotification(messageType) {
    checkDefined(messageType, 'messageType');
    return messageType === 'OversizedConfigurationItemChangeNotification';
}

// Get the configurationItem for the resource using the getResourceConfigHistory
 API.
async function getConfiguration(resourceType, resourceId, configurationCaptureTime,
 callback) {
    const input = { resourceType, resourceId, laterTime: new
 Date(configurationCaptureTime), limit: 1 };
    const command = new GetResourceConfigHistoryCommand(input);
    await configClient.send(command).then(
        (data) => {
            callback(null, data.configurationItems[0]);
        },
        (error) => {
            callback(error, null);
        }
    );

}

// Convert the oversized configuration item from the API model to the original
 invocation model.
function convertApiConfiguration(apiConfiguration) {
    apiConfiguration.awsAccountId = apiConfiguration.accountId;
    apiConfiguration.ARN = apiConfiguration.arn;
    apiConfiguration.configurationStateMd5Hash =
 apiConfiguration.configurationItemMD5Hash;
    apiConfiguration.configurationItemVersion = apiConfiguration.version;
    apiConfiguration.configuration = JSON.parse(apiConfiguration.configuration);
    if ({}.hasOwnProperty.call(apiConfiguration, 'relationships')) {
        for (let i = 0; i < apiConfiguration.relationships.length; i++) {
            apiConfiguration.relationships[i].name =
 apiConfiguration.relationships[i].relationshipName;
        }
    }
    return apiConfiguration;
}
```

```
// Based on the message type, get the configuration item either from the
 configurationItem object in the invoking event or with the getResourceConfigHistory
 API in the getConfiguration function.
async function getConfigurationItem(invokingEvent, callback) {
    checkDefined(invokingEvent, 'invokingEvent');
    if (isOverSizedChangeNotification(invokingEvent.messageType)) {
        const configurationItemSummary =
 checkDefined(invokingEvent.configurationItemSummary, 'configurationItemSummary');
        await getConfiguration(configurationItemSummary.resourceType,
 configurationItemSummary.resourceId,
 configurationItemSummary.configurationItemCaptureTime, (err, apiConfigurationItem)
 => {
            if (err) {
                callback(err);
            }
            const configurationItem = convertApiConfiguration(apiConfigurationItem);
            callback(null, configurationItem);
        });
    } else {
        checkDefined(invokingEvent.configurationItem, 'configurationItem');
        callback(null, invokingEvent.configurationItem);
    }
}

// Check whether the resource has been deleted. If the resource was deleted, then
 the evaluation returns not applicable.
function isApplicable(configurationItem, event) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(event, 'event');
    const status = configurationItem.configurationItemStatus;
    const eventLeftScope = event.eventLeftScope;
    return (status === 'OK' || status === 'ResourceDiscovered') && eventLeftScope
 === false;
}

// In this example, the resource is compliant if it is an instance and its type
 matches the type specified as the desired type.
// If the resource is not an instance, then this resource is not applicable.
function evaluateChangeNotificationCompliance(configurationItem, ruleParameters) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(configurationItem.configuration,
 'configurationItem.configuration');
    checkDefined(ruleParameters, 'ruleParameters');
```

```
    if (configurationItem.resourceType !== 'AWS::EC2::Instance') {
        return 'NOT_APPLICABLE';
    } else if (ruleParameters.desiredInstanceType ===
 configurationItem.configuration.instanceType) {
        return 'COMPLIANT';
    }
    return 'NON_COMPLIANT';
}

// Receives the event and context from AWS Lambda.
export const handler = async (event, context) => {
    checkDefined(event, 'event');
    const invokingEvent = JSON.parse(event.invokingEvent);
    const ruleParameters = JSON.parse(event.ruleParameters);
    await getConfigurationItem(invokingEvent, async (err, configurationItem) => {

        let compliance = 'NOT_APPLICABLE';
        let annotation = '';
        const putEvaluationsRequest = {};
        if (isApplicable(configurationItem, event)) {
            // Invoke the compliance checking function.
            compliance = evaluateChangeNotificationCompliance(configurationItem,
 ruleParameters);
            if (compliance === "NON_COMPLIANT") {
                annotation = "This is an annotation describing why the resource is
 not compliant.";
            }
        }
        // Initializes the request that contains the evaluation results.
        if (annotation) {
            putEvaluationsRequest.Evaluations = [
                {
                    ComplianceResourceType: configurationItem.resourceType,
                    ComplianceResourceId: configurationItem.resourceId,
                    ComplianceType: compliance,
                    OrderingTimestamp: new
 Date(configurationItem.configurationItemCaptureTime),
                    Annotation: annotation
                },
            ];
        } else {
            putEvaluationsRequest.Evaluations = [
                {
```

```
                    ComplianceResourceType: configurationItem.resourceType,
                    ComplianceResourceId: configurationItem.resourceId,
                    ComplianceType: compliance,
                    OrderingTimestamp: new
 Date(configurationItem.configurationItemCaptureTime),
                },
            ];
        }
        putEvaluationsRequest.ResultToken = event.resultToken;

        // Sends the evaluation results to AWS Config.
        await configClient.send(new PutEvaluationsCommand(putEvaluationsRequest));
    });
};
```

Operasi Fungsi

Fungsi melakukan operasi berikut saat runtime:

1. Fungsi berjalan ketika AWS Lambda melewati `event` objek ke `handler` fungsi. Dalam contoh ini, fungsi menerima `callback` parameter opsional, yang digunakan untuk mengembalikan informasi ke pemanggil. AWS Lambda juga melewati `context` objek, yang berisi informasi dan metode yang dapat digunakan fungsi saat berjalan. Perhatikan bahwa dalam versi Lambda yang lebih baru, konteks tidak lagi digunakan.
2. Fungsi memeriksa apakah `messageType` untuk acara tersebut adalah item konfigurasi atau item konfigurasi besar, dan kemudian mengembalikan item konfigurasi.
3. Handler memanggil `isApplicable` fungsi untuk menentukan apakah sumber daya telah dihapus.

   > **Note**
   >
   > Aturan pelaporan sumber daya yang dihapus harus mengembalikan hasil evaluasi untuk menghindari evaluasi aturan yang tidak perlu. `NOT_APPLICABLE`

4. Handler memanggil `evaluateChangeNotificationCompliance` fungsi dan meneruskan `configurationItem` dan `ruleParameters` objek yang AWS Config diterbitkan dalam acara tersebut.

   Fungsi pertama mengevaluasi apakah sumber daya adalah sebuah EC2 instance. Jika sumber daya bukan sebuah EC2 instance, fungsi mengembalikan nilai kepatuhan`NOT_APPLICABLE`.

Fungsi kemudian mengevaluasi apakah `instanceType` atribut dalam item konfigurasi sama dengan nilai `desiredInstanceType` parameter. Jika nilainya sama, fungsi kembali`COMPLIANT`. Jika nilainya tidak sama, fungsi kembali`NON_COMPLIANT`.

5. Handler bersiap untuk mengirim hasil evaluasi AWS Config dengan menginisialisasi objek. `putEvaluationsRequest` Objek ini mencakup `Evaluations` parameter, yang mengidentifikasi hasil kepatuhan, jenis sumber daya, dan ID sumber daya yang dievaluasi. `putEvaluationsRequest`Objek juga menyertakan token hasil dari acara, yang mengidentifikasi aturan dan acara untuk AWS Config.
6. Handler mengirimkan hasil evaluasi AWS Config dengan meneruskan objek ke `putEvaluations` metode `config` klien.

Example Function for Periodic Evaluations

AWS Config akan memanggil fungsi seperti contoh berikut untuk evaluasi berkala. Evaluasi periodik terjadi pada frekuensi yang Anda tentukan saat Anda menentukan aturan di AWS Config.

Jika Anda menggunakan AWS Config konsol untuk membuat aturan yang terkait dengan fungsi seperti contoh ini, pilih Periodik sebagai jenis pemicu. Jika Anda menggunakan AWS Config API atau AWS CLI membuat aturan, setel `MessageType` atribut ke`ScheduledNotification`.

Contoh ini memeriksa apakah jumlah total sumber daya tertentu melebihi maksimum yang ditentukan.

```
'use strict';
import { ConfigServiceClient, ListDiscoveredResourcesCommand,
 PutEvaluationsCommand } from "@aws-sdk/client-config-service";

const configClient = new ConfigServiceClient({});

// Receives the event and context from AWS Lambda.
export const handler = async (event, context, callback) => {
    // Parses the invokingEvent and ruleParameters values, which contain JSON
 objects passed as strings.
    var invokingEvent = JSON.parse(event.invokingEvent),
        ruleParameters = JSON.parse(event.ruleParameters),
        numberOfResources = 0;

    if (isScheduledNotification(invokingEvent) &&
 hasValidRuleParameters(ruleParameters, callback)) {
```

```
        await countResourceTypes(ruleParameters.applicableResourceType, "",
numberOfResources, async function (err, count) {
            if (err === null) {
                var putEvaluationsRequest;
                const compliance = evaluateCompliance(ruleParameters.maxCount,
count);
                var annotation = '';
                if (compliance === "NON_COMPLIANT") {
                    annotation = "Description of why the resource is not
compliant.";
                }
                // Initializes the request that contains the evaluation results.
                if (annotation) {
                    putEvaluationsRequest = {
                        Evaluations: [{
                            // Applies the evaluation result to the AWS account
published in the event.
                            ComplianceResourceType: 'AWS::::Account',
                            ComplianceResourceId: event.accountId,
                            ComplianceType: compliance,
                            OrderingTimestamp: new Date(),
                            Annotation: annotation
                        }],
                        ResultToken: event.resultToken
                    };
                } else {
                    putEvaluationsRequest = {
                        Evaluations: [{
                            // Applies the evaluation result to the AWS account
published in the event.
                            ComplianceResourceType: 'AWS::::Account',
                            ComplianceResourceId: event.accountId,
                            ComplianceType: compliance,
                            OrderingTimestamp: new Date()
                        }],
                        ResultToken: event.resultToken
                    };
                }

                // Sends the evaluation results to AWS Config.
                try {
                    await configClient.send(new
PutEvaluationsCommand(putEvaluationsRequest));
                }
```

```
                catch (e) {
                    callback(e, null);
                }
            } else {
                callback(err, null);
            }
        });
    } else {
        console.log("Invoked for a notification other than Scheduled Notification...
 Ignoring.");
    }
};

// Checks whether the invoking event is ScheduledNotification.
function isScheduledNotification(invokingEvent) {
    return (invokingEvent.messageType === 'ScheduledNotification');
}

// Checks the rule parameters to see if they are valid
function hasValidRuleParameters(ruleParameters, callback) {
    // Regular express to verify that applicable resource given is a resource type
    const awsResourcePattern = /^AWS::(\w*)::(\w*)$/;
    const isApplicableResourceType =
 awsResourcePattern.test(ruleParameters.applicableResourceType);
    // Check to make sure the maxCount in the parameters is an integer
    const maxCountIsInt = !isNaN(ruleParameters.maxCount) &&
 parseInt(Number(ruleParameters.maxCount)) == ruleParameters.maxCount && !
isNaN(parseInt(ruleParameters.maxCount, 10));
    if (!isApplicableResourceType) {
        callback("The applicableResourceType parameter is not a valid resource
 type.", null);
    }
    if (!maxCountIsInt) {
        callback("The maxCount parameter is not a valid integer.", null);
    }
    return isApplicableResourceType && maxCountIsInt;
}

// Checks whether the compliance conditions for the rule are violated.
function evaluateCompliance(maxCount, actualCount) {
    if (actualCount > maxCount) {
        return "NON_COMPLIANT";
    } else {
        return "COMPLIANT";
```

```
    }
}

// Counts the applicable resources that belong to the AWS account.
async function countResourceTypes(applicableResourceType, nextToken, count,
 callback) {
    const input = { resourceType: applicableResourceType, nextToken: nextToken };
    const command = new ListDiscoveredResourcesCommand(input);
    try {
        const response = await configClient.send(command);
        count = count + response.resourceIdentifiers.length;
        if (response.nextToken !== undefined && response.nextToken != null) {
            countResourceTypes(applicableResourceType, response.nextToken, count,
 callback);
        }
        callback(null, count);
    } catch (e) {
        callback(e, null);
    }
    return count;
}
```

Operasi Fungsi

Fungsi melakukan operasi berikut saat runtime:

1. Fungsi berjalan ketika AWS Lambda melewati `event` objek ke `handler` fungsi. Dalam contoh ini, fungsi menerima `callback` parameter opsional, yang digunakan untuk mengembalikan informasi ke pemanggil. AWS Lambda juga melewati `context` objek, yang berisi informasi dan metode yang dapat digunakan fungsi saat berjalan. Perhatikan bahwa dalam versi Lambda yang lebih baru, konteks tidak lagi digunakan.
2. Untuk menghitung sumber daya dari tipe yang ditentukan, handler memanggil `countResourceTypes` fungsi, dan melewati `applicableResourceType` parameter yang diterimanya dari acara tersebut. `countResourceTypes`Fungsi ini memanggil `listDiscoveredResources` metode `config` klien, yang mengembalikan daftar pengidentifikasi untuk sumber daya yang berlaku. Fungsi ini menggunakan panjang daftar ini untuk menentukan jumlah sumber daya yang berlaku, dan mengembalikan hitungan ini ke handler.
3. Handler bersiap untuk mengirim hasil evaluasi AWS Config dengan menginisialisasi objek. `putEvaluationsRequest` Objek ini mencakup `Evaluations` parameter, yang

mengidentifikasi hasil kepatuhan dan Akun AWS yang diterbitkan dalam acara tersebut. Anda dapat menggunakan `Evaluations` parameter untuk menerapkan hasilnya ke jenis sumber daya apa pun yang didukung oleh AWS Config. `putEvaluationsRequest`Objek juga menyertakan token hasil dari acara, yang mengidentifikasi aturan dan acara untuk AWS Config.

4. Di dalam `putEvaluationsRequest` objek, handler memanggil `evaluateCompliance` fungsi. Fungsi ini menguji apakah jumlah sumber daya yang berlaku melebihi maksimum yang ditetapkan ke `maxCount` parameter, yang disediakan oleh acara. Jika jumlah sumber daya melebihi maksimum, fungsi kembali`NON_COMPLIANT`. Jika jumlah sumber daya tidak melebihi maksimum, fungsi kembali`COMPLIANT`.
5. Handler mengirimkan hasil evaluasi AWS Config dengan meneruskan objek ke `putEvaluations` metode `config` klien.

Contoh AWS Lambda Fungsi untuk AWS Config Aturan (Python)

AWS Lambda menjalankan fungsi dalam menanggapi peristiwa yang diterbitkan oleh AWS layanan. Fungsi untuk aturan Lambda AWS Config Kustom menerima peristiwa yang diterbitkan oleh AWS Config, dan fungsi tersebut kemudian menggunakan data yang diterimanya dari acara dan diambil dari AWS Config API untuk mengevaluasi kepatuhan aturan. Operasi dalam fungsi untuk aturan Config berbeda tergantung pada apakah ia melakukan evaluasi yang dipicu oleh perubahan konfigurasi atau dipicu secara berkala.

Untuk informasi tentang pola umum dalam AWS Lambda fungsi, lihat Model Pemrograman di Panduan AWS Lambda Pengembang.

Example Function for Evaluations Triggered by Configuration Changes

AWS Config akan memanggil fungsi seperti contoh berikut ketika mendeteksi perubahan konfigurasi untuk sumber daya yang berada dalam cakupan aturan khusus.

Jika Anda menggunakan AWS Config konsol untuk membuat aturan yang terkait dengan fungsi seperti contoh ini, pilih Perubahan konfigurasi sebagai jenis pemicu. Jika Anda menggunakan AWS Config API atau AWS CLI untuk membuat aturan, atur `MessageType` atribut ke `ConfigurationItemChangeNotification` dan`OversizedConfigurationItemChangeNotification`. Pengaturan ini memungkinkan aturan Anda dipicu setiap kali AWS Config menghasilkan item konfigurasi atau item konfigurasi yang terlalu besar sebagai akibat dari perubahan sumber daya.

```
import botocore
```

```
import boto3
import json
import datetime

# Set to True to get the lambda to assume the Role attached on the Config Service
 (useful for cross-account).
ASSUME_ROLE_MODE = False

# This gets the client after assuming the Config service role
# either in the same AWS account or cross-account.
def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling
 the client.
    Keyword arguments:
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
    credentials = get_assume_role_credentials(event["executionRoleArn"])
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
                        aws_secret_access_key=credentials['SecretAccessKey'],
                        aws_session_token=credentials['SessionToken']
                       )

# Helper function used to validate input
def check_defined(reference, reference_name):
    if not reference:
        raise Exception('Error: ', reference_name, 'is not defined')
    return reference

# Check whether the message is OversizedConfigurationItemChangeNotification or not
def is_oversized_changed_notification(message_type):
    check_defined(message_type, 'messageType')
    return message_type == 'OversizedConfigurationItemChangeNotification'

# Get configurationItem using getResourceConfigHistory API
# in case of OversizedConfigurationItemChangeNotification
def get_configuration(resource_type, resource_id, configuration_capture_time):
    result = AWS_CONFIG_CLIENT.get_resource_config_history(
        resourceType=resource_type,
        resourceId=resource_id,
        laterTime=configuration_capture_time,
        limit=1)
```

```
    configurationItem = result['configurationItems'][0]
    return convert_api_configuration(configurationItem)

# Convert from the API model to the original invocation model
def convert_api_configuration(configurationItem):
    for k, v in configurationItem.items():
        if isinstance(v, datetime.datetime):
            configurationItem[k] = str(v)
    configurationItem['awsAccountId'] = configurationItem['accountId']
    configurationItem['ARN'] = configurationItem['arn']
    configurationItem['configurationStateMd5Hash'] =
 configurationItem['configurationItemMD5Hash']
    configurationItem['configurationItemVersion'] = configurationItem['version']
    configurationItem['configuration'] =
 json.loads(configurationItem['configuration'])
    if 'relationships' in configurationItem:
        for i in range(len(configurationItem['relationships'])):
            configurationItem['relationships'][i]['name'] =
 configurationItem['relationships'][i]['relationshipName']
    return configurationItem

# Based on the type of message get the configuration item
# either from configurationItem in the invoking event
# or using the getResourceConfigHistory API in getConfiguration function.
def get_configuration_item(invokingEvent):
    check_defined(invokingEvent, 'invokingEvent')
    if is_oversized_changed_notification(invokingEvent['messageType']):
        configurationItemSummary =
 check_defined(invokingEvent['configurationItemSummary'],
 'configurationItemSummary')
        return get_configuration(configurationItemSummary['resourceType'],
 configurationItemSummary['resourceId'],
 configurationItemSummary['configurationItemCaptureTime'])
    return check_defined(invokingEvent['configurationItem'], 'configurationItem')

# Check whether the resource has been deleted. If it has, then the evaluation is
 unnecessary.
def is_applicable(configurationItem, event):
    try:
        check_defined(configurationItem, 'configurationItem')
        check_defined(event, 'event')
    except:
        return True
    status = configurationItem['configurationItemStatus']
```

```
    eventLeftScope = event['eventLeftScope']
    if status == 'ResourceDeleted':
        print("Resource Deleted, setting Compliance Status to NOT_APPLICABLE.")
    return (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope

def get_assume_role_credentials(role_arn):
    sts_client = boto3.client('sts')
    try:
        assume_role_response = sts_client.assume_role(RoleArn=role_arn,
 RoleSessionName="configLambdaExecution")
        return assume_role_response['Credentials']
    except botocore.exceptions.ClientError as ex:
        # Scrub error message for any internal account info leaks
        if 'AccessDenied' in ex.response['Error']['Code']:
            ex.response['Error']['Message'] = "AWS Config does not have permission
 to assume the IAM role."
        else:
            ex.response['Error']['Message'] = "InternalError"
            ex.response['Error']['Code'] = "InternalError"
        raise ex

def evaluate_change_notification_compliance(configuration_item, rule_parameters):
    check_defined(configuration_item, 'configuration_item')
    check_defined(configuration_item['configuration'],
 'configuration_item[\'configuration\']')
    if rule_parameters:
        check_defined(rule_parameters, 'rule_parameters')

    if (configuration_item['resourceType'] != 'AWS::EC2::Instance'):
        return 'NOT_APPLICABLE'

    elif rule_parameters.get('desiredInstanceType'):
        if (configuration_item['configuration']['instanceType'] in
 rule_parameters['desiredInstanceType']):
            return 'COMPLIANT'
    return 'NON_COMPLIANT'

def lambda_handler(event, context):

    global AWS_CONFIG_CLIENT

    check_defined(event, 'event')
    invoking_event = json.loads(event['invokingEvent'])
    rule_parameters = {}
```

```
    if 'ruleParameters' in event:
        rule_parameters = json.loads(event['ruleParameters'])

    compliance_value = 'NOT_APPLICABLE'

    AWS_CONFIG_CLIENT = get_client('config', event)
    configuration_item = get_configuration_item(invoking_event)
    if is_applicable(configuration_item, event):
        compliance_value = evaluate_change_notification_compliance(
                configuration_item, rule_parameters)

    response = AWS_CONFIG_CLIENT.put_evaluations(
       Evaluations=[
           {
               'ComplianceResourceType': invoking_event['configurationItem']
['resourceType'],
               'ComplianceResourceId': invoking_event['configurationItem']
['resourceId'],
               'ComplianceType': compliance_value,
               'OrderingTimestamp': invoking_event['configurationItem']
['configurationItemCaptureTime']
           },
       ],
       ResultToken=event['resultToken'])
```

Operasi Fungsi

Fungsi melakukan operasi berikut saat runtime:

1. Fungsi berjalan ketika AWS Lambda melewati `event` objek ke `handler` fungsi. Dalam contoh ini, fungsi menerima `callback` parameter opsional, yang digunakan untuk mengembalikan informasi ke pemanggil. AWS Lambda juga melewati `context` objek, yang berisi informasi dan metode yang dapat digunakan fungsi saat berjalan. Perhatikan bahwa dalam versi Lambda yang lebih baru, konteks tidak lagi digunakan.
2. Fungsi memeriksa apakah `messageType` untuk acara tersebut adalah item konfigurasi atau item konfigurasi besar, dan kemudian mengembalikan item konfigurasi.
3. Handler memanggil `isApplicable` fungsi untuk menentukan apakah sumber daya telah dihapus.

> **Note**
>
> Aturan pelaporan sumber daya yang dihapus harus mengembalikan hasil evaluasi untuk menghindari evaluasi aturan yang tidak perlu. `NOT_APPLICABLE`

4. Handler memanggil `evaluateChangeNotificationCompliance` fungsi dan meneruskan `configurationItem` dan `ruleParameters` objek yang AWS Config diterbitkan dalam acara tersebut.

   Fungsi pertama mengevaluasi apakah sumber daya adalah sebuah EC2 instance. Jika sumber daya bukan sebuah EC2 instance, fungsi mengembalikan nilai kepatuhan`NOT_APPLICABLE`.

   Fungsi kemudian mengevaluasi apakah `instanceType` atribut dalam item konfigurasi sama dengan nilai `desiredInstanceType` parameter. Jika nilainya sama, fungsi kembali`COMPLIANT`. Jika nilainya tidak sama, fungsi kembali`NON_COMPLIANT`.
5. Handler bersiap untuk mengirim hasil evaluasi AWS Config dengan menginisialisasi objek. `putEvaluationsRequest` Objek ini mencakup `Evaluations` parameter, yang mengidentifikasi hasil kepatuhan, jenis sumber daya, dan ID sumber daya yang dievaluasi. `putEvaluationsRequest`Objek juga menyertakan token hasil dari acara, yang mengidentifikasi aturan dan acara untuk AWS Config.
6. Handler mengirimkan hasil evaluasi AWS Config dengan meneruskan objek ke `putEvaluations` metode `config` klien.

Example Function for Periodic Evaluations

AWS Config akan memanggil fungsi seperti contoh berikut untuk evaluasi berkala. Evaluasi periodik terjadi pada frekuensi yang Anda tentukan saat Anda menentukan aturan di AWS Config.

Jika Anda menggunakan AWS Config konsol untuk membuat aturan yang terkait dengan fungsi seperti contoh ini, pilih Periodik sebagai jenis pemicu. Jika Anda menggunakan AWS Config API atau AWS CLI membuat aturan, setel `MessageType` atribut ke`ScheduledNotification`.

```
import botocore
import boto3
import json
import datetime
```

```
# Set to True to get the lambda to assume the Role attached on the Config Service
 (useful for cross-account).
ASSUME_ROLE_MODE = False
DEFAULT_RESOURCE_TYPE = 'AWS::::Account'

# This gets the client after assuming the Config service role
# either in the same AWS account or cross-account.
def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling
 the client.
    Keyword arguments:
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
    credentials = get_assume_role_credentials(event["executionRoleArn"])
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
                        aws_secret_access_key=credentials['SecretAccessKey'],
                        aws_session_token=credentials['SessionToken']
                       )

def get_assume_role_credentials(role_arn):
    sts_client = boto3.client('sts')
    try:
        assume_role_response = sts_client.assume_role(RoleArn=role_arn,
 RoleSessionName="configLambdaExecution")
        return assume_role_response['Credentials']
    except botocore.exceptions.ClientError as ex:
        # Scrub error message for any internal account info leaks
        if 'AccessDenied' in ex.response['Error']['Code']:
            ex.response['Error']['Message'] = "AWS Config does not have permission
 to assume the IAM role."
        else:
            ex.response['Error']['Message'] = "InternalError"
            ex.response['Error']['Code'] = "InternalError"
        raise ex

# Check whether the message is a ScheduledNotification or not.
def is_scheduled_notification(message_type):
    return message_type == 'ScheduledNotification'

def count_resource_types(applicable_resource_type, next_token, count):
```

```
    resource_identifier =
 AWS_CONFIG_CLIENT.list_discovered_resources(resourceType=applicable_resource_type,
 nextToken=next_token)
    updated = count + len(resource_identifier['resourceIdentifiers']);
    return updated

# Evaluates the configuration items in the snapshot and returns the compliance value
 to the handler.
def evaluate_compliance(max_count, actual_count):
    return 'NON_COMPLIANT' if int(actual_count) > int(max_count) else 'COMPLIANT'

def evaluate_parameters(rule_parameters):
    if 'applicableResourceType' not in rule_parameters:
        raise ValueError('The parameter with "applicableResourceType" as key must be
 defined.')
    if not rule_parameters['applicableResourceType']:
        raise ValueError('The parameter "applicableResourceType" must have a defined
 value.')
    return rule_parameters

# This generate an evaluation for config
def build_evaluation(resource_id, compliance_type, event,
 resource_type=DEFAULT_RESOURCE_TYPE, annotation=None):
    """Form an evaluation as a dictionary. Usually suited to report on scheduled
 rules.
    Keyword arguments:
    resource_id -- the unique id of the resource to report
    compliance_type -- either COMPLIANT, NON_COMPLIANT or NOT_APPLICABLE
    event -- the event variable given in the lambda handler
    resource_type -- the CloudFormation resource type (or AWS::::Account) to report
 on the rule (default DEFAULT_RESOURCE_TYPE)
    annotation -- an annotation to be added to the evaluation (default None)
    """
    eval_cc = {}
    if annotation:
        eval_cc['Annotation'] = annotation
    eval_cc['ComplianceResourceType'] = resource_type
    eval_cc['ComplianceResourceId'] = resource_id
    eval_cc['ComplianceType'] = compliance_type
    eval_cc['OrderingTimestamp'] = str(json.loads(event['invokingEvent'])
['notificationCreationTime'])
    return eval_cc

def lambda_handler(event, context):
```

```
    global AWS_CONFIG_CLIENT

    evaluations = []
    rule_parameters = {}
    resource_count = 0
    max_count = 0

    invoking_event = json.loads(event['invokingEvent'])
    if 'ruleParameters' in event:
        rule_parameters = json.loads(event['ruleParameters'])
        valid_rule_parameters = evaluate_parameters(rule_parameters)

    compliance_value = 'NOT_APPLICABLE'

    AWS_CONFIG_CLIENT = get_client('config', event)
    if is_scheduled_notification(invoking_event['messageType']):
        result_resource_count =
 count_resource_types(valid_rule_parameters['applicableResourceType'], '',
 resource_count)

    if valid_rule_parameters.get('maxCount'):
        max_count = valid_rule_parameters['maxCount']

    compliance_value = evaluate_compliance(max_count, result_resource_count)
    evaluations.append(build_evaluation(event['accountId'], compliance_value, event,
 resource_type=DEFAULT_RESOURCE_TYPE))
    response = AWS_CONFIG_CLIENT.put_evaluations(Evaluations=evaluations,
 ResultToken=event['resultToken'])
```

Operasi Fungsi

Fungsi melakukan operasi berikut saat runtime:

1. Fungsi berjalan ketika AWS Lambda melewati `event` objek ke `handler` fungsi. Dalam contoh ini, fungsi menerima `callback` parameter opsional, yang digunakan untuk mengembalikan informasi ke pemanggil. AWS Lambda juga melewati `context` objek, yang berisi informasi dan metode yang dapat digunakan fungsi saat berjalan. Perhatikan bahwa dalam versi Lambda yang lebih baru, konteks tidak lagi digunakan.
2. Untuk menghitung sumber daya dari tipe yang ditentukan, handler memanggil `countResourceTypes` fungsi, dan melewati `applicableResourceType` parameter yang diterimanya dari acara tersebut. `countResourceTypes`Fungsi ini memanggil

`listDiscoveredResources` metode `config` klien, yang mengembalikan daftar pengidentifikasi untuk sumber daya yang berlaku. Fungsi ini menggunakan panjang daftar ini untuk menentukan jumlah sumber daya yang berlaku, dan mengembalikan hitungan ini ke handler.

3. Handler bersiap untuk mengirim hasil evaluasi AWS Config dengan menginisialisasi objek. `putEvaluationsRequest` Objek ini mencakup `Evaluations` parameter, yang mengidentifikasi hasil kepatuhan dan Akun AWS yang diterbitkan dalam acara tersebut. Anda dapat menggunakan `Evaluations` parameter untuk menerapkan hasilnya ke jenis sumber daya apa pun yang didukung oleh AWS Config. `putEvaluationsRequest`Objek juga menyertakan token hasil dari acara, yang mengidentifikasi aturan dan acara untuk AWS Config.
4. Di dalam `putEvaluationsRequest` objek, handler memanggil `evaluateCompliance` fungsi. Fungsi ini menguji apakah jumlah sumber daya yang berlaku melebihi maksimum yang ditetapkan ke `maxCount` parameter, yang disediakan oleh acara. Jika jumlah sumber daya melebihi maksimum, fungsi kembali`NON_COMPLIANT`. Jika jumlah sumber daya tidak melebihi maksimum, fungsi kembali`COMPLIANT`.
5. Handler mengirimkan hasil evaluasi AWS Config dengan meneruskan objek ke `putEvaluations` metode `config` klien.

Contoh Acara untuk AWS Config Aturan

Ketika pemicu aturan terjadi, AWS Config memanggil AWS Lambda fungsi aturan dengan menerbitkan peristiwa. Kemudian AWS Lambda mengeksekusi fungsi dengan meneruskan event ke handler fungsi.

Example Event for Evaluations Triggered by Configuration Changes

AWS Config menerbitkan peristiwa ketika mendeteksi perubahan konfigurasi untuk sumber daya yang berada dalam lingkup aturan. Contoh peristiwa berikut menunjukkan bahwa aturan dipicu oleh perubahan konfigurasi untuk sebuah EC2 instance.

```
{
    "invokingEvent": "{\"configurationItem\":{\"configurationItemCaptureTime
\":\"2016-02-17T01:36:34.043Z\",\"awsAccountId\":\"123456789012\",
\"configurationItemStatus\":\"OK\",\"resourceId\":\"i-00000000\",\"ARN
\":\"arn:aws:ec2:us-east-2:123456789012:instance/i-00000000\",\"awsRegion
\":\"us-east-2\",\"availabilityZone\":\"us-east-2a\",\"resourceType\":
\"AWS::EC2::Instance\",\"tags\":{\"Foo\":\"Bar\"},\"relationships\":[{\"resourceId
\":\"eipalloc-00000000\",\"resourceType\":\"AWS::EC2::EIP\",\"name\":\"Is
```

```
 attached to ElasticIp\"}],\"configuration\":{\"foo\":\"bar\"}},\"messageType\":
\"ConfigurationItemChangeNotification\"}",
    "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
    "resultToken": "myResultToken",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
    "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
    "configRuleName": "change-triggered-config-rule",
    "configRuleId": "config-rule-0123456",
    "accountId": "123456789012",
    "version": "1.0"
}
```

Example Event for Evaluations Triggered by Oversized Configuration Changes

Beberapa perubahan sumber daya menghasilkan item konfigurasi yang terlalu besar. Contoh peristiwa berikut menunjukkan bahwa aturan dipicu oleh perubahan konfigurasi yang terlalu besar untuk sebuah EC2 instance.

```
{
        "invokingEvent": "{\"configurationItemSummary\": {\"changeType\":
 \"UPDATE\",\"configurationItemVersion\": \"1.2\",\"configurationItemCaptureTime
\":\"2016-10-06T16:46:16.261Z\",\"configurationStateId\": 0,\"awsAccountId
\":\"123456789012\",\"configurationItemStatus\": \"OK\",\"resourceType
\": \"AWS::EC2::Instance\",\"resourceId\":\"i-00000000\",\"resourceName
\":null,\"ARN\":\"arn:aws:ec2:us-west-2:123456789012:instance/i-00000000\",
\"awsRegion\": \"us-west-2\",\"availabilityZone\":\"us-west-2a\",
\"configurationStateMd5Hash\":\"8f1ee69b287895a0f8bc5753eca68e96\",
\"resourceCreationTime\":\"2016-10-06T16:46:10.489Z\"},\"messageType\":
\"OversizedConfigurationItemChangeNotification\"}",
        "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
        "resultToken": "myResultToken",
        "eventLeftScope": false,
        "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
        "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-ec2-managed-instance-inventory",
        "configRuleName": "change-triggered-config-rule",
        "configRuleId": "config-rule-0123456",
        "accountId": "123456789012",
        "version": "1.0"
    }
```

Example Event for Evaluations Triggered by Periodic Frequency

AWS Config menerbitkan acara saat mengevaluasi sumber daya Anda pada frekuensi yang Anda tentukan (seperti setiap 24 jam). Contoh peristiwa berikut menunjukkan bahwa aturan dipicu oleh frekuensi periodik.

```
{
    "invokingEvent": "{\"awsAccountId\":\"123456789012\",\"notificationCreationTime
\":\"2016-07-13T21:50:00.373Z\",\"messageType\":\"ScheduledNotification\",
\"recordVersion\":\"1.0\"}",
    "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
    "resultToken": "myResultToken",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
    "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
    "configRuleName": "periodic-config-rule",
    "configRuleId": "config-rule-6543210",
    "accountId": "123456789012",
    "version": "1.0"
}
```

Atribut Acara

Objek JSON untuk AWS Config acara berisi atribut berikut:

`invokingEvent`

Peristiwa yang memicu evaluasi untuk suatu aturan. Jika acara dipublikasikan sebagai respons terhadap perubahan konfigurasi sumber daya, nilai untuk atribut ini adalah string yang berisi JSON `configurationItem` atau `configurationItemSummary` (untuk item konfigurasi berukuran besar). Item konfigurasi mewakili status sumber daya pada saat AWS Config mendeteksi perubahan. Untuk contoh item konfigurasi, lihat output yang dihasilkan oleh `get-resource-config-history` AWS CLI perintah diMelihat Riwayat Konfigurasi.

Jika acara diterbitkan untuk evaluasi berkala, nilainya adalah string yang berisi objek JSON. Objek tersebut mencakup informasi tentang evaluasi yang dipicu.

Untuk setiap jenis acara, fungsi harus mengurai string dengan parser JSON untuk dapat mengevaluasi isinya, seperti yang ditunjukkan pada contoh Node.js berikut:

```
var invokingEvent = JSON.parse(event.invokingEvent);
```

`ruleParameters`

Pasangan kunci/nilai yang diproses fungsi sebagai bagian dari logika evaluasinya. Anda menentukan parameter saat menggunakan AWS Config konsol untuk membuat aturan Lambda Kustom. Anda juga dapat menentukan parameter dengan `InputParameters` atribut dalam permintaan `PutConfigRule` AWS Config API atau `put-config-rule` AWS CLI perintah.

Kode JSON untuk parameter terkandung dalam string, sehingga fungsi harus mengurai string dengan parser JSON untuk dapat mengevaluasi isinya, seperti yang ditunjukkan dalam contoh Node.js berikut:

```
var ruleParameters = JSON.parse(event.ruleParameters);
```

`resultToken`

Token yang harus diteruskan oleh fungsi AWS Config dengan `PutEvaluations` panggilan.

`eventLeftScope`

Nilai Boolean yang menunjukkan apakah AWS sumber daya yang akan dievaluasi telah dihapus dari lingkup aturan. Jika nilainya`true`, fungsi menunjukkan bahwa evaluasi dapat diabaikan dengan meneruskan `NOT_APPLICABLE` sebagai nilai untuk `ComplianceType` atribut dalam `PutEvaluations` panggilan.

`executionRoleArn`

ARN dari peran IAM yang ditugaskan untuk. AWS Config

`configRuleArn`

ARN yang AWS Config ditugaskan untuk aturan.

`configRuleName`

Nama yang Anda tetapkan untuk aturan yang menyebabkan AWS Config untuk mempublikasikan acara dan memanggil fungsi.

`configRuleId`

ID yang AWS Config ditetapkan untuk aturan.

`accountId`

ID Akun AWS yang memiliki aturan.

`version`

Nomor versi yang ditetapkan oleh AWS. Versi akan bertambah jika AWS menambahkan atribut ke AWS Config acara. Jika fungsi memerlukan atribut yang hanya dalam peristiwa yang cocok atau melebihi versi tertentu, maka fungsi tersebut dapat memeriksa nilai atribut ini.

Versi saat ini untuk AWS Config acara adalah 1.0.

Mengelola Sumber Daya yang Dihapus untuk AWS Config Aturan Lambda Kustom

Aturan pelaporan sumber daya yang dihapus harus mengembalikan hasil evaluasi untuk menghindari evaluasi aturan yang tidak perlu. `NOT_APPLICABLE`

Saat Anda menghapus sumber daya, AWS Config buat `configurationItem` dengan `ResourceDeleted` untuk file`configurationItemStatus`. Anda dapat menggunakan metadata ini untuk memeriksa apakah aturan melaporkan sumber daya yang dihapus. Untuk informasi selengkapnya tentang item konfigurasi, lihat Konsep | Item Konfigurasi.

Sertakan cuplikan kode berikut untuk memeriksa sumber daya yang dihapus dan setel hasil evaluasi aturan lambda AWS Config kustom `NOT_APPLICABLE` jika melaporkan sumber daya yang dihapus:

Custom Lambda Rules (Node.js)

```
// Check whether the resource has been deleted. If the resource was deleted, then
 the evaluation returns not applicable.
function isApplicable(configurationItem, event) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(event, 'event');
    const status = configurationItem.configurationItemStatus;
    const eventLeftScope = event.eventLeftScope;
    return (status === 'OK' || status === 'ResourceDiscovered') && eventLeftScope
 === false;
}
```

Custom Lambda Rules (Python)

```
# Check whether the resource has been deleted. If the resource was deleted, then the
 evaluation returns not applicable.
```

```
def is_applicable(configurationItem, event):
    try:
        check_defined(configurationItem, 'configurationItem')
        check_defined(event, 'event')
    except:
        return True
    status = configurationItem['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']
    if status == 'ResourceDeleted':
        print("Resource Deleted, setting Compliance Status to NOT_APPLICABLE.")
    return (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope
```

> **Note**
>
> AWS Config aturan terkelola dan aturan kebijakan AWS Config khusus menangani perilaku ini secara default.
> Jika Anda membuat aturan lambd AWS Config kustom dengan Python menggunakan AWS Config Development Kit (RDK) AWS Config dan Development Kit Library RDKlib (), class Evaluator yang diimpor akan memeriksa perilaku ini. Untuk informasi tentang cara menulis aturan dengan RDK dan RDKlib, lihat Menulis aturan dengan RDK dan. RDKlib

Aturan Terkait Layanan AWS Config

AWS Config Aturan terkait layanan adalah jenis aturan AWS Config terkelola unik yang mendukung AWS layanan lain untuk membuat AWS Config aturan di akun Anda. Aturan terkait layanan telah ditentukan sebelumnya untuk menyertakan semua izin yang diperlukan untuk memanggil AWS layanan lain atas nama Anda. Aturan-aturan ini mirip dengan standar yang direkomendasikan oleh AWS layanan Anda Akun AWS untuk verifikasi kepatuhan.

AWS Config Aturan terkait layanan ini dimiliki oleh tim AWS layanan. Tim AWS layanan membuat aturan ini di Anda Akun AWS. Anda memiliki akses hanya-baca ke aturan ini. Anda tidak dapat mengedit atau menghapus aturan ini jika Anda berlangganan AWS layanan yang terkait dengan aturan ini.

Aturan terkait layanan dan AWS Command Line Interface

Dengan AWS CLI, akses PutConfigRule, DeleteConfigRule, dan DeleteEvaluationResults APIs kembali ditolak dengan pesan kesalahan berikut:

```
INSUFFICIENT_SLCR_PERMISSIONS = "An AWS service owns
ServiceLinkedConfigRule. You do not have permissions to take action on this
rule."
```

Aturan terkait layanan dan konsol AWS Config

Di AWS Config konsol, AWS Config aturan terkait layanan terlihat di halaman Aturan. Tombol Edit dan Hapus hasil berwarna abu-abu di konsol untuk membatasi Anda mengedit aturan. Anda dapat melihat detail aturan dengan memilih aturan.

Aturan terkait layanan, tindakan remediasi, dan paket kesesuaian

Untuk menambahkan tindakan remediasi ke aturan terkait layanan dalam paket kesesuaian, Anda perlu menambahkan tindakan remediasi ke templat paket kesesuaian itu sendiri, lalu memperbarui paket kesesuaian dengan templat yang diperbarui. Untuk informasi tentang memperbarui paket kesesuaian, lihat Menerapkan Paket Kesesuaian (Konsol), Menerapkan Paket Kesesuaian (), dan Mengelola Paket Kesesuaian Organisasi.AWS CLI

Mengedit dan menghapus aturan terkait layanan

Untuk mengedit atau menghapus aturan terkait layanan, hubungi AWS layanan yang membuat aturan. Misalnya, untuk aturan terkait layanan yang dibuat oleh AWS Security Hub, Anda dapat menghapus aturan terkait layanan dengan mengikuti langkah-langkah ini di Panduan AWS Security Hub Pengguna: Menonaktifkan standar keamanan.

Mengelola AWS Config Aturan di Semua Akun di Organisasi Anda

> **Important**
>
> Aturan organisasi hanya dapat dibuat menggunakan API atau CLI. Operasi ini tidak didukung di AWS Config konsol.

AWS Config memungkinkan Anda untuk mengelola AWS Config aturan di semua Akun AWS dalam suatu organisasi. Anda dapat:

- Buat, perbarui, dan hapus AWS Config aturan secara terpusat di semua akun di organisasi Anda.
- Terapkan seperangkat AWS Config aturan umum di semua akun dan tentukan akun di mana AWS Config aturan tidak boleh dibuat.

- Gunakan APIs dari akun manajemen AWS Organizations untuk menegakkan tata kelola dengan memastikan bahwa AWS Config aturan yang mendasarinya tidak dapat dimodifikasi oleh akun anggota organisasi Anda.

Pertimbangan

Untuk penyebaran di berbagai wilayah

Panggilan API untuk menerapkan aturan dan paket kesesuaian di seluruh akun adalah spesifik Wilayah. AWS Di tingkat organisasi, Anda perlu mengubah konteks panggilan API ke wilayah lain jika ingin menerapkan aturan di wilayah lain. Misalnya, untuk menerapkan aturan di AS Timur (Virginia N.), ubah wilayah ke AS Timur (Virginia N.) dan kemudian hubungi. `PutOrganizationConfigRule`

Untuk akun dalam suatu organisasi

Jika akun baru bergabung dengan organisasi, aturan atau paket kesesuaian diterapkan ke akun tersebut. Ketika akun meninggalkan organisasi, aturan atau paket kesesuaian akan dihapus.

Jika Anda menerapkan aturan organisasi atau paket kesesuaian di akun administrator organisasi, lalu membuat administrator yang didelegasikan dan menerapkan aturan organisasi atau paket kesesuaian di akun administrator yang didelegasikan, Anda tidak akan dapat melihat aturan organisasi atau paket kesesuaian di akun administrator organisasi dari akun administrator yang didelegasikan atau melihat aturan organisasi atau paket kesesuaian dalam akun administrator yang didelegasikan dari akun administrator organisasi. The DescribeOrganizationConfigRulesdan hanya DescribeOrganizationConformancePacks APIs dapat melihat dan berinteraksi dengan sumber daya terkait organisasi yang digunakan dari dalam akun yang memanggilnya. APIs

Coba lagi mekanisme untuk akun baru yang ditambahkan ke organisasi

Penerapan aturan organisasi yang ada dan paket kesesuaian hanya akan dicoba ulang selama 7 jam setelah akun ditambahkan ke organisasi Anda jika perekam tidak tersedia. Anda diharapkan untuk membuat perekam jika tidak ada dalam waktu 7 jam setelah menambahkan akun ke organisasi Anda.

Akun manajemen organisasi, administrator yang didelegasikan, dan peran terkait layanan

Jika Anda menggunakan akun manajemen organisasi dan ingin menggunakan administrator yang didelegasikan untuk penerapan organisasi, ketahuilah bahwa tidak AWS Config akan secara otomatis membuat peran terkait layanan (SLR). Anda harus secara manual membuat peran terkait layanan (SLR) secara terpisah menggunakan IAM.

Jika Anda tidak memiliki SLR untuk akun manajemen Anda, Anda tidak akan dapat menyebarkan sumber daya ke akun itu dari akun administrator yang didelegasikan. Anda masih dapat menerapkan AWS Config aturan ke akun anggota dari manajemen dan akun administrator yang didelegasikan. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan di Panduan Pengguna AWS Identity and Access Management (IAM).

Deployment

Untuk informasi tentang cara mengintegrasikan AWS Config dengan AWS Organizations, lihat AWS Config dan AWS Organizations di Panduan AWS Organizations Pengguna. Pastikan AWS Config perekaman aktif sebelum Anda menggunakan yang berikut ini APIs untuk mengelola AWS Config aturan di semua Akun AWS dalam organisasi:

- PutOrganizationConfigRule, menambahkan atau memperbarui aturan konfigurasi organisasi untuk seluruh organisasi Anda mengevaluasi apakah AWS sumber daya Anda sesuai dengan konfigurasi yang Anda inginkan.
- DescribeOrganizationConfigRules, mengembalikan daftar aturan konfigurasi organisasi.
- GetOrganizationConfigRuleDetailedStatus, mengembalikan status terperinci untuk setiap akun anggota dalam organisasi untuk aturan konfigurasi organisasi tertentu.
- GetOrganizationCustomRulePolicy, mengembalikan definisi kebijakan yang berisi logika untuk aturan kebijakan kustom konfigurasi organisasi Anda.
- DescribeOrganizationConfigRuleStatuses, menyediakan status penerapan aturan konfigurasi organisasi untuk organisasi.
- DeleteOrganizationConfigRule, menghapus aturan konfigurasi organisasi yang ditentukan dan semua hasil evaluasinya dari semua akun anggota di organisasi itu.

Support Wilayah

Menerapkan AWS Config Aturan di seluruh akun anggota di AWS Organisasi didukung di Wilayah berikut.

Nama Wilayah	Wilayah	Titik Akhir	Protokol	
AS Timur (Ohio)	us–east-2	config.us-east-2.amazonaws.com	HTTPS	

Nama Wilayah	Wilayah	Titik Akhir	Protokol
AS Timur (Virginia Utara)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
AS Barat (California Utara)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
AS Barat (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
Afrika (Cape Town)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asia Pasifik (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asia Pasifik (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asia Pasifik (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asia Pasifik (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Asia Pasifik (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pasifik (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia Pasifik (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia Pasifik (Singapura)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pasifik (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Kanada (Pusat)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Kanada Barat (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Eropa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Eropa (Irlandia)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Eropa (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Eropa (Milan)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Eropa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Eropa (Spanyol)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Eropa (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Eropa (Zürich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Timur Tengah (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Timur Tengah (UAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Amerika Selatan (Sao Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (AS-Timur)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (AS-Barat)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Menambahkan AWS Config Aturan

Anda dapat menggunakan AWS Config konsol atau AWS SDKs untuk menambahkan aturan.

Topik

- Menambahkan Aturan (Konsol)
- Menambahkan Aturan (AWS SDKs)

Menambahkan Aturan (Konsol)

Halaman Aturan menunjukkan aturan Anda dan hasil kepatuhannya saat ini dalam sebuah tabel. Hasil untuk setiap aturan adalah Mengevaluasi... sampai AWS Config selesai mengevaluasi sumber daya Anda terhadap aturan. Anda dapat memperbarui hasil dengan tombol refresh. Saat AWS Config menyelesaikan evaluasi, Anda dapat melihat aturan dan jenis sumber daya yang sesuai atau tidak sesuai. Untuk informasi selengkapnya, lihat Melihat Informasi Kepatuhan dan Hasil Evaluasi untuk AWS Sumber Daya Anda dengan AWS Config.

> **Note**
>
> Saat Anda menambahkan aturan baru, AWS Config evaluasi sumber daya yang berlaku dalam inventaris sumber daya Anda, termasuk sumber daya yang direkam sebelumnya. Misalnya, jika Anda merekam `AWS::IoT::Policy` sumber daya tetapi kemudian mengecualikannya dari rekaman, AWS Config menyimpan item konfigurasi awal (CIs) dalam inventaris Anda. Meskipun AWS Config tidak lagi memperbarui ini CIs ketika jenis sumber daya terkait mereka dikecualikan dari rekaman, itu mempertahankan status rekaman terakhir mereka dan mengevaluasi mereka ketika Anda menambahkan aturan yang berlaku.
> AWS Config tidak mengevaluasi sumber daya yang tidak ada dalam inventaris sumber daya. Misalnya, jika Anda menambahkan amplify-branch-tagged aturan tetapi tidak merekam dan tidak pernah merekam `AWS::Amplify::Branch` sumber daya, tidak AWS Config dapat mengevaluasi apakah AWS Amplify cabang di akun Anda sesuai atau tidak sesuai.
> Untuk informasi selengkapnya, lihat Merekam AWS Sumber Daya dengan AWS Config.

Menambahkan aturan

Untuk menambahkan aturan

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Di AWS Management Console menu, verifikasi bahwa pemilih wilayah diatur ke wilayah yang mendukung AWS Config aturan. Untuk daftar wilayah yang didukung, lihat AWS Config Wilayah dan Titik Akhir di. Referensi Umum Amazon Web Services
3. Di navigasi kiri, pilih Aturan.
4. Pada halaman Aturan, pilih Tambahkan aturan.
5. Pada halaman Tentukan tipe aturan, tentukan jenis aturan dengan menyelesaikan langkah-langkah berikut:

    a. Ketik kolom pencarian untuk memfilter daftar aturan terkelola berdasarkan nama aturan, deskripsi, dan label. Misalnya, ketik EC2untuk mengembalikan aturan yang mengevaluasi jenis EC2 sumber daya atau ketik periodik untuk mengembalikan aturan yang dipicu secara berkala.

    b. Anda juga dapat membuat aturan kustom Anda sendiri. Pilih Buat aturan kustom menggunakan Lambda atau Buat aturan kustom menggunakan Guard, dan ikuti prosedur di

Membuat Aturan AWS Config Lambda Kustom atau Membuat AWS Config Aturan Kebijakan Kustom.

6. Pada halaman Konfigurasi aturan, konfigurasikan aturan Anda dengan menyelesaikan langkah-langkah berikut:

   a. Untuk Nama, ketik nama unik untuk aturan.

   b. Untuk Deskripsi, ketikkan deskripsi untuk aturan.

   c. Untuk mode Evaluasi, pilih kapan dalam proses pembuatan dan manajemen sumber daya Anda AWS Config ingin mengevaluasi sumber daya Anda. Tergantung pada aturan, AWS Config dapat mengevaluasi konfigurasi sumber daya Anda sebelum sumber daya telah digunakan, setelah sumber daya telah digunakan, atau keduanya.

      i. Pilih Aktifkan evaluasi proaktif untuk memungkinkan Anda menjalankan evaluasi pada setelan konfigurasi sumber daya Anda sebelum diterapkan.

         Setelah mengaktifkan evaluasi proaktif, Anda dapat menggunakan StartResourceEvaluationAPI dan GetResourceEvaluationSummaryAPI untuk memeriksa apakah sumber daya yang Anda tentukan dalam perintah ini akan ditandai sebagai NON_COMPLIANT oleh aturan proaktif di akun Anda di Wilayah Anda.

         Untuk informasi selengkapnya tentang penggunaan perintah ini, lihat Mengevaluasi Sumber Daya Anda dengan AWS Config Aturan. Untuk daftar aturan terkelola yang mendukung evaluasi proaktif, lihat Daftar Aturan AWS Config Terkelola menurut Mode Evaluasi.

      ii. Pilih Aktifkan evaluasi detektif untuk mengevaluasi pengaturan konfigurasi sumber daya yang ada.

         Untuk evaluasi detektif, ada dua jenis pemicu: Ketika konfigurasi berubah dan Periodik.

         A. Jika tipe pemicu untuk aturan Anda menyertakan perubahan Konfigurasi, tentukan salah satu opsi berikut untuk Lingkup perubahan yang digunakan untuk AWS Config memanggil fungsi Lambda Anda:

            - Sumber Daya — Saat sumber daya yang cocok dengan jenis sumber daya yang ditentukan, atau pengenal tipe plus, dibuat, diubah, atau dihapus.
            - Tag — Ketika sumber daya dengan tag yang ditentukan dibuat, diubah, atau dihapus.

- Semua perubahan — Ketika sumber daya yang direkam oleh AWS Config dibuat, diubah, atau dihapus.

  AWS Config menjalankan evaluasi saat mendeteksi perubahan pada sumber daya yang cocok dengan cakupan aturan. Anda dapat menggunakan ruang lingkup untuk menentukan sumber daya mana yang memulai evaluasi.

B. Jika tipe pemicu untuk aturan Anda menyertakan Periodik, tentukan Frekuensi yang digunakan untuk AWS Config memanggil fungsi Lambda Anda.

d. Untuk Parameter, Anda dapat menyesuaikan nilai untuk kunci yang disediakan jika aturan Anda menyertakan parameter. Parameter adalah atribut yang harus dipatuhi oleh sumber daya Anda sebelum dianggap sesuai dengan aturan.

7. Pada halaman Tinjau dan buat, tinjau semua pilihan Anda sebelum menambahkan aturan ke halaman Anda Akun AWS. Jika aturan Anda tidak berfungsi seperti yang diharapkan, Anda mungkin melihat salah satu dari berikut ini untuk Kepatuhan:

   - Tidak ada hasil yang dilaporkan - AWS Config mengevaluasi sumber daya Anda terhadap aturan. Aturan tidak berlaku untuk AWS sumber daya dalam ruang lingkupnya, sumber daya yang ditentukan dihapus, atau hasil evaluasi dihapus. Untuk mendapatkan hasil evaluasi, perbarui aturan, ubah cakupannya, atau pilih Evaluasi ulang.

     Pesan ini juga dapat muncul jika aturan tidak melaporkan hasil evaluasi.
   - Tidak ada sumber daya dalam ruang lingkup - AWS Config tidak dapat mengevaluasi AWS sumber daya Anda yang direkam terhadap aturan ini karena tidak ada sumber daya Anda yang berada dalam cakupan aturan. Untuk mendapatkan hasil evaluasi, edit aturan dan ubah cakupannya, atau tambahkan sumber daya AWS Config untuk direkam menggunakan halaman Pengaturan.
   - Evaluasi gagal - Untuk informasi yang dapat membantu Anda menentukan masalah, pilih nama aturan untuk membuka halaman detailnya dan lihat pesan galat.

Menambahkan Aturan (AWS SDKs)

Menambahkan aturan

Contoh kode berikut menunjukkan cara menggunakan`PutConfigRule`.

CLI

AWS CLI

Untuk menambahkan aturan Config AWS terkelola

Perintah berikut menyediakan kode JSON untuk menambahkan aturan Config AWS terkelola:

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.jsonadalah` file JSON yang berisi konfigurasi aturan:

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

Untuk `ComplianceResourceTypes` atribut, kode JSON ini membatasi cakupan ke sumber daya `AWS::EC2::Instance` tipe, jadi AWS Config EC2 hanya akan mengevaluasi instance terhadap aturan. Karena aturan adalah aturan terkelola, `Owner` atribut disetel ke`AWS`, dan `SourceIdentifier` atribut diatur ke pengidentifikasi aturan,`REQUIRED_TAGS`. Untuk `InputParameters` atribut, kunci tag yang dibutuhkan aturan, `CostCenter` dan`Owner`, ditentukan.

Jika perintah berhasil, AWS Config tidak mengembalikan output. Untuk memverifikasi konfigurasi aturan, jalankan describe-config-rules perintah, dan tentukan nama aturan.

Untuk menambahkan aturan Config terkelola pelanggan

Perintah berikut menyediakan kode JSON untuk menambahkan aturan Config terkelola pelanggan:

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

`InstanceTypesAreT2micro.jsonadalah` file JSON yang berisi konfigurasi aturan:

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

Untuk `ComplianceResourceTypes` atribut, kode JSON ini membatasi cakupan ke sumber daya `AWS::EC2::Instance` tipe, jadi AWS Config EC2 hanya akan mengevaluasi instance terhadap aturan. Karena aturan ini adalah aturan yang dikelola pelanggan, `Owner` atribut disetel ke`CUSTOM_LAMBDA`, dan `SourceIdentifier` atribut disetel ke ARN dari fungsi Lambda AWS . `SourceDetailsObjek` diperlukan. Parameter yang ditentukan untuk `InputParameters` atribut diteruskan ke fungsi AWS Lambda saat AWS Config memanggilnya untuk mengevaluasi sumber daya terhadap aturan.

Jika perintah berhasil, AWS Config tidak mengembalikan output. Untuk memverifikasi konfigurasi aturan, jalankan describe-config-rules perintah, dan tentukan nama aturan.

- Untuk detail API, lihat PutConfigRuledi Referensi AWS CLI Perintah.

Python

SDK untuk Python (Boto3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
 publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
```

```
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- Untuk detail API, lihat PutConfigRuledi AWS SDK for Python (Boto3) Referensi API.

Memperbarui AWS Config Aturan

Anda dapat menggunakan AWS Config konsol atau AWS SDKs untuk memperbarui aturan Anda.

Topik

- Memperbarui Aturan (Konsol)
- Memperbarui Aturan (AWS SDKs)

Memperbarui Aturan (Konsol)

Halaman Aturan menunjukkan aturan Anda dan hasil kepatuhannya saat ini dalam sebuah tabel. Hasil untuk setiap aturan adalah Mengevaluasi... sampai AWS Config selesai mengevaluasi sumber daya Anda terhadap aturan. Anda dapat memperbarui hasil dengan tombol refresh. Saat AWS Config menyelesaikan evaluasi, Anda dapat melihat aturan dan jenis sumber daya yang sesuai atau tidak sesuai. Untuk informasi selengkapnya, lihat Melihat Informasi Kepatuhan dan Hasil Evaluasi untuk AWS Sumber Daya Anda dengan AWS Config.

Memperbarui aturan

Cara memperbarui aturan

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.

2. Di AWS Management Console menu, verifikasi bahwa pemilih wilayah diatur ke wilayah yang mendukung AWS Config aturan. Untuk daftar wilayah yang didukung, lihat AWS Config Wilayah dan Titik Akhir di. Referensi Umum Amazon Web Services
3. Di navigasi kiri, pilih Aturan.
4. Pilih aturan dan Edit aturan untuk aturan yang ingin Anda perbarui.
5. Ubah pengaturan pada halaman Edit aturan untuk mengubah aturan Anda sesuai kebutuhan.
6. Pilih Simpan.

Memperbarui Aturan (AWS SDKs)

Memperbarui aturan

Jika Anda memperbarui aturan yang Anda tambahkan sebelumnya, Anda dapat menentukan aturan dengan `ConfigRuleName`, `ConfigRuleId`, atau `ConfigRuleArn` atau dalam tipe data `ConfigRule` yang Anda gunakan dalam permintaan ini. Anda menggunakan `PutConfigRule` perintah yang sama yang Anda gunakan saat menambahkan aturan.

Contoh kode berikut menunjukkan cara menggunakan`PutConfigRule`.

CLI

AWS CLI

Untuk menambahkan aturan Config AWS terkelola

Perintah berikut menyediakan kode JSON untuk menambahkan aturan Config AWS terkelola:

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.json`adalah file JSON yang berisi konfigurasi aturan:

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
```

```
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

Untuk `ComplianceResourceTypes` atribut, kode JSON ini membatasi cakupan sumber daya `AWS::EC2::Instance` tipe, jadi AWS Config EC2 hanya akan mengevaluasi instance terhadap aturan. Karena aturan adalah aturan terkelola, `Owner` atribut diatur ke`AWS`, dan `SourceIdentifier` atribut diatur ke pengidentifikasi aturan,`REQUIRED_TAGS`. Untuk `InputParameters` atribut, kunci tag yang dibutuhkan aturan, `CostCenter` dan`Owner`, ditentukan.

Jika perintah berhasil, AWS Config tidak mengembalikan output. Untuk memverifikasi konfigurasi aturan, jalankan describe-config-rules perintah, dan tentukan nama aturan.

Untuk menambahkan aturan Config terkelola pelanggan

Perintah berikut menyediakan kode JSON untuk menambahkan aturan Config terkelola pelanggan:

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

`InstanceTypesAreT2micro.json`adalah file JSON yang berisi konfigurasi aturan:

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
```

```
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

Untuk `ComplianceResourceTypes` atribut, kode JSON ini membatasi cakupan sumber daya `AWS::EC2::Instance` tipe, jadi AWS Config EC2 hanya akan mengevaluasi instance terhadap aturan. Karena aturan ini adalah aturan yang dikelola pelanggan, `Owner` atribut disetel ke`CUSTOM_LAMBDA`, dan `SourceIdentifier` atribut disetel ke ARN dari fungsi Lambda AWS . `SourceDetails`Objek diperlukan. Parameter yang ditentukan untuk `InputParameters` atribut diteruskan ke fungsi AWS Lambda saat AWS Config memanggilnya untuk mengevaluasi sumber daya terhadap aturan.

Jika perintah berhasil, AWS Config tidak mengembalikan output. Untuk memverifikasi konfigurasi aturan, jalankan describe-config-rules perintah, dan tentukan nama aturan.

- Untuk detail API, lihat PutConfigRuledi Referensi AWS CLI Perintah.

Python

SDK untuk Python (Boto3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
```

```
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- Untuk detail API, lihat PutConfigRuledi AWS SDK for Python (Boto3) Referensi API.

Menghapus Aturan AWS Config

Anda dapat menggunakan AWS Config konsol atau AWS SDKs untuk menghapus aturan Anda.

Topik

- Pertimbangan
- Menghapus Aturan (Konsol)
- Menghapus Aturan ()AWS SDKs

Pertimbangan

Rekomendasi: Pertimbangkan untuk mengecualikan jenis **`AWS::Config::ResourceCompliance`** sumber daya dari rekaman sebelum menghapus aturan

Menghapus aturan membuat item konfigurasi (CIs) untuk `AWS::Config::ResourceCompliance` itu dapat memengaruhi biaya Anda untuk perekam konfigurasi. Jika Anda menghapus aturan yang mengevaluasi sejumlah besar jenis sumber daya, ini dapat menyebabkan lonjakan jumlah CIs yang direkam.

Untuk menghindari biaya terkait, Anda dapat memilih untuk menonaktifkan perekaman untuk jenis `AWS::Config::ResourceCompliance` sumber daya sebelum menghapus aturan, dan mengaktifkan kembali perekaman setelah aturan dihapus.

Namun, karena menghapus aturan adalah proses asinkron, mungkin perlu satu jam atau lebih untuk menyelesaikannya. Selama perekaman dinonaktifkan`AWS::Config::ResourceCompliance`, evaluasi aturan tidak akan dicatat dalam riwayat sumber daya terkait.

Menghapus Aturan (Konsol)

Halaman Aturan menunjukkan aturan Anda dan hasil kepatuhannya saat ini dalam sebuah tabel. Hasil untuk setiap aturan adalah Mengevaluasi... sampai AWS Config selesai mengevaluasi sumber daya Anda terhadap aturan. Anda dapat memperbarui hasilnya dengan tombol refresh. Saat AWS Config menyelesaikan evaluasi, Anda dapat melihat aturan dan jenis sumber daya yang sesuai atau tidak sesuai. Untuk informasi selengkapnya, lihat Melihat Informasi Kepatuhan dan Hasil Evaluasi untuk AWS Sumber Daya Anda dengan AWS Config.

> **Note**
>
> AWS Config mengevaluasi hanya jenis sumber daya yang direkam. Misalnya, jika Anda menambahkan aturan berkemampuan cloudtrail tetapi tidak merekam jenis sumber daya CloudTrail jejak, tidak AWS Config dapat mengevaluasi apakah jejak di akun Anda sesuai

atau tidak sesuai. Untuk informasi selengkapnya, lihat Merekam AWS Sumber Daya dengan AWS Config.

Menghapus aturan

Untuk menghapus aturan

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Di AWS Management Console menu, verifikasi bahwa pemilih wilayah diatur ke wilayah yang mendukung AWS Config aturan. Untuk daftar wilayah yang didukung, lihat AWS Config Wilayah dan Titik Akhir di. Referensi Umum Amazon Web Services
3. Di navigasi kiri, pilih Aturan.
4. Pilih aturan dari tabel yang ingin Anda hapus.
5. Dari daftar dropdown Tindakan, pilih Hapus aturan.
6. Saat diminta, ketik “Hapus” (peka huruf besar/kecil) lalu pilih Hapus.

Menghapus Aturan ()AWS SDKs

Menghapus aturan

Contoh kode berikut menunjukkan cara menggunakan`DeleteConfigRule`.

CLI

AWS CLI

Untuk menghapus aturan AWS Config

Perintah berikut menghapus aturan AWS Config bernama: `MyConfigRule`

```
aws configservice delete-config-rule --config-rule-name MyConfigRule
```

- Untuk detail API, lihat DeleteConfigRuledi Referensi AWS CLI Perintah.

Python

SDK untuk Python (Boto3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def delete_config_rule(self, rule_name):
        """
        Delete the specified rule.

        :param rule_name: The name of the rule to delete.
        """
        try:
            self.config_client.delete_config_rule(ConfigRuleName=rule_name)
            logger.info("Deleted rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't delete rule %s.", rule_name)
            raise
```

- Untuk detail API, lihat DeleteConfigRuledi AWS SDK for Python (Boto3) Referensi API.

Melihat Detail dan Informasi Kepatuhan untuk AWS Config Aturan Anda

> **Important**
>
> Untuk pelaporan yang akurat tentang status kepatuhan, Anda harus mencatat jenis `AWS::Config::ResourceCompliance` sumber daya. Untuk informasi selengkapnya, lihat Merekam AWS Sumber Daya.

Anda dapat menggunakan AWS Config konsol atau AWS SDKs untuk melihat aturan Anda.

Topik

- Aturan Melihat (Konsol)
- Aturan Melihat (AWS SDKs)

Aturan Melihat (Konsol)

Halaman Aturan menunjukkan aturan Anda dan hasil kepatuhannya saat ini dalam sebuah tabel. Hasil untuk setiap aturan adalah Mengevaluasi... sampai AWS Config selesai mengevaluasi sumber daya Anda terhadap aturan. Anda dapat memperbarui hasil dengan tombol refresh. Saat AWS Config menyelesaikan evaluasi, Anda dapat melihat aturan dan jenis sumber daya yang sesuai atau tidak sesuai. Untuk informasi selengkapnya, lihat Melihat Informasi Kepatuhan dan Hasil Evaluasi untuk AWS Sumber Daya Anda dengan AWS Config.

> **Note**
>
> AWS Config mengevaluasi hanya jenis sumber daya yang direkam. Misalnya, jika Anda menambahkan aturan berkemampuan cloudtrail tetapi tidak merekam jenis sumber daya CloudTrail jejak, tidak AWS Config dapat mengevaluasi apakah jejak di akun Anda sesuai atau tidak sesuai. Untuk informasi selengkapnya, lihat Merekam AWS Sumber Daya dengan AWS Config.

Aturan tampilan

Untuk melihat aturan Anda

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Di AWS Management Console menu, verifikasi bahwa pemilih wilayah diatur ke wilayah yang mendukung AWS Config aturan. Untuk daftar wilayah yang didukung, lihat AWS Config Wilayah dan Titik Akhir di. Referensi Umum Amazon Web Services
3. Di navigasi kiri, pilih Aturan.
4. Halaman Aturan menunjukkan semua aturan yang saat ini ada di Anda Akun AWS. Ini mencantumkan nama, tindakan remediasi terkait, dan status kepatuhan setiap aturan.
   - Pilih Tambahkan aturan untuk memulai membuat aturan.
   - Pilih aturan untuk melihat pengaturannya, atau pilih aturan dan Lihat detail.
   - Lihat status kepatuhan aturan saat mengevaluasi sumber daya Anda.
   - Pilih aturan dan Edit aturan untuk mengubah pengaturan konfigurasi aturan dan menetapkan tindakan remediasi untuk aturan yang tidak sesuai.

Aturan Melihat (AWS SDKs)

Melihat detail untuk aturan Anda

Contoh kode berikut menunjukkan cara menggunakan`DescribeConfigRules`.

CLI

AWS CLI

Untuk mendapatkan detail tentang aturan AWS Config

Perintah berikut mengembalikan rincian untuk aturan AWS Config bernama: `InstanceTypesAreT2micro`

```
aws configservice describe-config-rules --config-rule-
names InstanceTypesAreT2micro
```

Output:

```
{
    "ConfigRules": [
        {
            "ConfigRuleState": "ACTIVE",
            "Description": "Evaluates whether EC2 instances are the t2.micro
 type.",
            "ConfigRuleName": "InstanceTypesAreT2micro",
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "Source": {
                "Owner": "CUSTOM_LAMBDA",
                "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
                "SourceDetails": [
                    {
                        "EventSource": "aws.config",
                        "MessageType": "ConfigurationItemChangeNotification"
                    }
                ]
            },
            "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}",
            "Scope": {
                "ComplianceResourceTypes": [
                    "AWS::EC2::Instance"
                ]
            },
            "ConfigRuleId": "config-rule-abcdef"
        }
    ]
}
```

- Untuk detail API, lihat DescribeConfigRulesdi Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Contoh ini mencantumkan aturan konfigurasi untuk akun, dengan properti yang dipilih.

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

Output:

```
ConfigRuleName                                     ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                     ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                              config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                                config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required         config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- Untuk detail API, lihat DescribeConfigRulesdi Referensi Alat AWS untuk PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Contoh ini mencantumkan aturan konfigurasi untuk akun, dengan properti yang dipilih.

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

Output:

```
ConfigRuleName                                     ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                     ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                              config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                                config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
```

```
autoscaling-group-elb-healthcheck-required        config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- Untuk detail API, lihat DescribeConfigRulesdi Referensi Alat AWS untuk PowerShell Cmdlet (V5).

Python

SDK untuk Python (Boto3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def describe_config_rule(self, rule_name):
        """
        Gets data for the specified rule.

        :param rule_name: The name of the rule to retrieve.
        :return: The rule data.
        """
        try:
            response = self.config_client.describe_config_rules(
                ConfigRuleNames=[rule_name]
            )
            rule = response["ConfigRules"]
```

```
            logger.info("Got data for rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't get data for rule %s.", rule_name)
            raise
        else:
            return rule
```

- Untuk detail API, lihat DescribeConfigRulesdi AWS SDK for Python (Boto3) Referensi API.

Melihat informasi kepatuhan untuk aturan Anda

Contoh kode berikut menunjukkan cara menggunakan`DescribeComplianceByConfigRule`.

CLI

AWS CLI

Untuk mendapatkan informasi kepatuhan untuk aturan AWS Config

Perintah berikut menampilkan informasi kepatuhan untuk setiap aturan AWS Config yang dilanggar oleh satu atau beberapa sumber daya: AWS

```
aws configservice describe-compliance-by-config-rule --compliance-
types NON_COMPLIANT
```

Dalam output, nilai untuk setiap `CappedCount` atribut menunjukkan berapa banyak sumber daya yang tidak sesuai dengan aturan terkait. Misalnya, output berikut menunjukkan bahwa 3 sumber daya tidak sesuai dengan aturan bernama`InstanceTypesAreT2micro`.

Output:

```
{
    "ComplianceByConfigRules": [
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
```

```
            },
            "ConfigRuleName": "InstanceTypesAreT2micro"
        },
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "RequiredTagsForVolumes"
        }
    ]
}
```

- Untuk detail API, lihat DescribeComplianceByConfigRuledi Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Contoh ini mengambil rincian kepatuhan untuk aturan ebs-optimized-instance, yang tidak ada hasil evaluasi saat ini untuk aturan, sehingga mengembalikan INSUFFICIENT_DATA

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

Output:

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

Contoh 2: Contoh ini mengembalikan jumlah sumber daya yang tidak sesuai untuk aturan ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK.

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

Output:

```
CapExceeded CappedCount
----------- -----------
False       2
```

- Untuk detail API, lihat DescribeComplianceByConfigRuledi Referensi Alat AWS untuk PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Contoh ini mengambil rincian kepatuhan untuk aturan ebs-optimized-instance, yang tidak ada hasil evaluasi saat ini untuk aturan, sehingga mengembalikan INSUFFICIENT_DATA

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

Output:

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

Contoh 2: Contoh ini mengembalikan jumlah sumber daya yang tidak sesuai untuk aturan ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK.

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

Output:

```
CapExceeded CappedCount
----------- -----------
False       2
```

- Untuk detail API, lihat DescribeComplianceByConfigRuledi Referensi Alat AWS untuk PowerShell Cmdlet (V5).

Melihat ringkasan kepatuhan untuk aturan Anda

Contoh kode berikut menunjukkan cara menggunakan`GetComplianceSummaryByConfigRule`.

CLI

AWS CLI

Untuk mendapatkan ringkasan kepatuhan untuk aturan AWS Config

Perintah berikut mengembalikan jumlah aturan yang sesuai dan nomor yang tidak sesuai:

```
aws configservice get-compliance-summary-by-config-rule
```

Dalam output, nilai untuk setiap `CappedCount` atribut menunjukkan berapa banyak aturan yang sesuai atau tidak sesuai.

Output:

```
{
    "ComplianceSummary": {
        "NonCompliantResourceCount": {
            "CappedCount": 3,
            "CapExceeded": false
        },
        "ComplianceSummaryTimestamp": 1452204131.493,
        "CompliantResourceCount": {
            "CappedCount": 2,
            "CapExceeded": false
        }
    }
}
```

- Untuk detail API, lihat GetComplianceSummaryByConfigRuledi Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Contoh ini mengembalikan jumlah aturan Config yang tidak sesuai.

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

Output:

```
CapExceeded CappedCount
----------- -----------
False       9
```

- Untuk detail API, lihat GetComplianceSummaryByConfigRuledi Referensi Alat AWS untuk PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Contoh ini mengembalikan jumlah aturan Config yang tidak sesuai.

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

Output:

```
CapExceeded CappedCount
----------- -----------
False       9
```

- Untuk detail API, lihat GetComplianceSummaryByConfigRuledi Referensi Alat AWS untuk PowerShell Cmdlet (V5).

Melihat hasil evaluasi untuk aturan Anda

Contoh kode berikut menunjukkan cara menggunakan`GetComplianceDetailsByConfigRule`.

CLI

AWS CLI

Untuk mendapatkan hasil evaluasi untuk aturan AWS Config

Perintah berikut mengembalikan hasil evaluasi untuk semua sumber daya yang tidak sesuai dengan aturan AWS Config bernama: `InstanceTypesAreT2micro`

```
aws configservice get-compliance-details-by-config-rule --config-rule-
name InstanceTypesAreT2micro --compliance-types NON_COMPLIANT
```

Output:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-2a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.18,
            "ConfigRuleInvokedTime": 1450314642.902,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-3a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.346,
            "ConfigRuleInvokedTime": 1450314643.124,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
```

```
}
```

- Untuk detail API, lihat GetComplianceDetailsByConfigRuledi Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Contoh ini memperoleh hasil evaluasi untuk aturan access-keys-rotated dan mengembalikan output yang dikelompokkan berdasarkan tipe kepatuhan

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

Output:

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

Contoh 2: Contoh ini menanyakan detail kepatuhan access-keys-rotated untuk aturan sumber daya COMPLIANT.

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

Output:

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- Untuk detail API, lihat GetComplianceDetailsByConfigRuledi Referensi Alat AWS untuk PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Contoh ini memperoleh hasil evaluasi untuk aturan access-keys-rotated dan mengembalikan output yang dikelompokkan berdasarkan tipe kepatuhan

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

Output:

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

Contoh 2: Contoh ini menanyakan detail kepatuhan access-keys-rotated untuk aturan sumber daya COMPLIANT.

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

Output:

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- Untuk detail API, lihat GetComplianceDetailsByConfigRuledi Referensi Alat AWS untuk PowerShell Cmdlet (V5).

Mengaktifkan Evaluasi Proaktif untuk Aturan AWS Config

Anda dapat menggunakan AWS Config konsol atau AWS SDKs untuk mengaktifkan aturan evaluasi proaktif. Untuk daftar jenis sumber daya dan aturan terkelola yang mendukung evaluasi proaktif, lihat Komponen Aturan | Mode Evaluasi.

Topik

- Mengaktifkan Evaluasi Proaktif (Konsol)
- Mengaktifkan Evaluasi Proaktif ()AWS SDKs

Mengaktifkan Evaluasi Proaktif (Konsol)

Halaman Aturan menunjukkan aturan Anda dan hasil kepatuhannya saat ini dalam sebuah tabel. Hasil untuk setiap aturan adalah Mengevaluasi... sampai AWS Config selesai mengevaluasi sumber daya Anda terhadap aturan. Anda dapat memperbarui hasil dengan tombol refresh.

Saat AWS Config menyelesaikan evaluasi, Anda dapat melihat aturan dan jenis sumber daya yang sesuai atau tidak sesuai. Untuk informasi selengkapnya, lihat Melihat Informasi Kepatuhan dan Hasil Evaluasi untuk AWS Sumber Daya Anda dengan AWS Config.

> **Note**
>
> AWS Config mengevaluasi hanya jenis sumber daya yang direkam. Misalnya, jika Anda menambahkan aturan berkemampuan cloudtrail tetapi tidak merekam jenis sumber daya CloudTrail jejak, tidak AWS Config dapat mengevaluasi apakah jejak di akun Anda sesuai atau tidak sesuai. Untuk informasi selengkapnya, lihat Merekam AWS Sumber Daya dengan AWS Config.

Mengaktifkan evaluasi proaktif

Anda dapat menggunakan evaluasi proaktif untuk mengevaluasi sumber daya sebelum digunakan. Ini memungkinkan Anda untuk mengevaluasi apakah satu set properti sumber daya, jika digunakan untuk mendefinisikan AWS sumber daya, akan COMPLIANT atau NON_COMPLIANT mengingat seperangkat aturan proaktif yang Anda miliki di akun Anda di Wilayah Anda.

Skema tipe Resource menyatakan properti sumber daya. Anda dapat menemukan skema jenis sumber daya di "ekstensi AWS publik" di dalam AWS CloudFormation registri atau dengan CLI commmand berikut:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

Untuk informasi selengkapnya, lihat Mengelola ekstensi melalui referensi AWS CloudFormation registri dan AWS sumber daya serta tipe properti di Panduan AWS CloudFormation Pengguna.

> **Note**
>
> Aturan proaktif tidak memulihkan sumber daya yang ditandai sebagai NON_COMPLIANT atau mencegahnya diterapkan.

Untuk mengaktifkan evaluasi proaktif

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Di AWS Management Console menu, verifikasi bahwa pemilih Wilayah diatur ke Wilayah yang mendukung AWS Config aturan. Untuk daftar AWS Wilayah yang didukung, lihat AWS Config Wilayah dan Titik Akhir di. Referensi Umum Amazon Web Services
3. Di navigasi kiri, pilih Aturan. Untuk daftar aturan terkelola yang mendukung evaluasi proaktif, lihat Daftar Aturan AWS Config Terkelola menurut Mode Evaluasi.
4. Pilih aturan, lalu pilih Edit aturan untuk aturan yang ingin Anda perbarui.
5. Untuk mode Evaluasi, pilih Aktifkan evaluasi proaktif untuk memungkinkan Anda menjalankan evaluasi pada pengaturan konfigurasi sumber daya Anda sebelum dikerahkan.
6. Pilih Simpan.

Setelah mengaktifkan evaluasi proaktif, Anda dapat menggunakan StartResourceEvaluationAPI dan GetResourceEvaluationSummaryAPI untuk memeriksa apakah sumber daya yang Anda tentukan dalam perintah ini akan ditandai sebagai NON_COMPLIANT oleh aturan proaktif di akun Anda di Wilayah Anda.

Misalnya, mulai dengan StartResourceEvaluation API:

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

Anda harus menerima `ResourceEvaluationId` dalam output:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Kemudian, gunakan `ResourceEvaluationId` dengan GetResourceEvaluationSummary API untuk memeriksa hasil evaluasi:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

Anda harus menerima output yang mirip dengan yang berikut ini:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

Untuk melihat informasi tambahan tentang hasil evaluasi, seperti aturan yang menandai sumber daya sebagai NON_COMPLIANT, gunakan API. GetComplianceDetailsByResource

Mengaktifkan Evaluasi Proaktif ()AWS SDKs

Mengaktifkan evaluasi proaktif ()AWS CLI

Anda dapat menggunakan evaluasi proaktif untuk mengevaluasi sumber daya sebelum digunakan. Ini memungkinkan Anda untuk mengevaluasi apakah satu set properti sumber daya, jika digunakan untuk mendefinisikan AWS sumber daya, akan COMPLIANT atau NON_COMPLIANT mengingat seperangkat aturan proaktif yang Anda miliki di akun Anda di Wilayah Anda.

Skema tipe Resource menyatakan properti sumber daya. Anda dapat menemukan skema jenis sumber daya di "ekstensi AWS publik" di dalam AWS CloudFormation registri atau dengan CLI commmand berikut:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

Untuk informasi selengkapnya, lihat Mengelola ekstensi melalui referensi AWS CloudFormation registri dan AWS sumber daya serta tipe properti di Panduan AWS CloudFormation Pengguna.

> **Note**
>
> Aturan proaktif tidak memulihkan sumber daya yang ditandai sebagai NON_COMPLIANT atau mencegahnya diterapkan.

Untuk mengaktifkan evaluasi proaktif

Gunakan `put-config-rule`perintah dan aktifkan `PROACTIVE` untuk`EvaluationModes`.

Setelah Anda mengaktifkan evaluasi proaktif, Anda dapat menggunakan perintah CLI dan get-resource-evaluation-summaryperintah start-resource-evaluationCLI untuk memeriksa apakah sumber daya yang Anda tentukan dalam perintah ini akan ditandai sebagai NON_COMPLIANT oleh aturan proaktif di akun Anda di Wilayah Anda.

Misalnya, mulailah dengan start-resource-evaluation perintah:

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

Anda harus menerima `ResourceEvaluationId` dalam output:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
```

```
}
```

Kemudian, gunakan `ResourceEvaluationId` with get-resource-evaluation-summary untuk memeriksa hasil evaluasi:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

Anda harus menerima output yang mirip dengan yang berikut ini:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

Untuk melihat informasi tambahan tentang hasil evaluasi, seperti aturan yang menandai sumber daya sebagai NON_COMPLIANT, gunakan perintah get-compliance-details-by -resource CLI.

> **Note**
>
> Untuk daftar aturan terkelola yang mendukung evaluasi proaktif, lihat Daftar Aturan AWS Config Terkelola menurut Mode Evaluasi.

Mengaktifkan evaluasi proaktif (API)

Anda dapat menggunakan evaluasi proaktif untuk mengevaluasi sumber daya sebelum digunakan. Ini memungkinkan Anda untuk mengevaluasi apakah satu set properti sumber daya, jika digunakan untuk mendefinisikan AWS sumber daya, akan COMPLIANT atau NON_COMPLIANT mengingat seperangkat aturan proaktif yang Anda miliki di akun Anda di Wilayah Anda.

Skema tipe Resource menyatakan properti sumber daya. Anda dapat menemukan skema jenis sumber daya di "ekstensi AWS publik" di dalam AWS CloudFormation registri atau dengan CLI commmand berikut:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

Untuk informasi selengkapnya, lihat Mengelola ekstensi melalui referensi AWS CloudFormation registri dan AWS sumber daya serta tipe properti di Panduan AWS CloudFormation Pengguna.

> **Note**
>
> Aturan proaktif tidak memulihkan sumber daya yang ditandai sebagai NON_COMPLIANT atau mencegahnya diterapkan.

Untuk mengaktifkan evaluasi proaktif untuk suatu aturan

Gunakan PutConfigRuletindakan dan aktifkan `PROACTIVE` untuk`EvaluationModes`.

Setelah mengaktifkan evaluasi proaktif, Anda dapat menggunakan StartResourceEvaluationAPI dan GetResourceEvaluationSummaryAPI untuk memeriksa apakah sumber daya yang Anda tentukan dalam perintah ini akan ditandai sebagai NON_COMPLIANT oleh aturan proaktif di akun Anda di Wilayah Anda. Misalnya, mulai dengan StartResourceEvaluation API:

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

Anda harus menerima `ResourceEvaluationId` dalam output:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Kemudian, gunakan `ResourceEvaluationId` dengan GetResourceEvaluationSummary API untuk memeriksa hasil evaluasi:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

Anda harus menerima output yang mirip dengan yang berikut ini:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

Untuk melihat informasi tambahan tentang hasil evaluasi, seperti aturan yang menandai sumber daya sebagai NON_COMPLIANT, gunakan API. GetComplianceDetailsByResource

> **Note**
>
> Untuk daftar aturan terkelola yang mendukung evaluasi proaktif, lihat Daftar Aturan AWS Config Terkelola menurut Mode Evaluasi.

Mengirim Evaluasi Aturan ke Security Hub

Setelah menambahkan AWS Config aturan, Anda juga dapat mengirim evaluasi aturan ke AWS Security Hub. Integrasi antara AWS Config dan Security Hub memungkinkan Anda melakukan triase dan memulihkan evaluasi aturan bersama kesalahan konfigurasi dan masalah keamanan lainnya.

Kirim Evaluasi Aturan ke Security Hub

Untuk mengirim evaluasi aturan ke Security Hub, Anda harus terlebih dahulu menyiapkan AWS Security Hub dan AWS Config, lalu menambahkan setidaknya satu aturan AWS Config terkelola atau kustom. Setelah ini, AWS Config segera mulai mengirim evaluasi aturan ke Security Hub. Security Hub memperkaya evaluasi aturan dan mengubahnya menjadi temuan Security Hub.

Untuk informasi selengkapnya tentang integrasi ini, lihat Integrasi AWS Layanan yang Tersedia di Panduan AWS Security Hub Pengguna.

Mengevaluasi Sumber Daya Anda dengan Aturan AWS Config

Saat Anda membuat aturan khusus atau menggunakan aturan terkelola, AWS Config evaluasi sumber daya Anda terhadap aturan tersebut. Anda dapat menjalankan evaluasi berdasarkan permintaan untuk sumber daya yang bertentangan dengan aturan Anda. Misalnya, ini berguna saat Anda membuat aturan khusus dan ingin memeriksa apakah mengevaluasi sumber daya Anda dengan benar atau untuk mengidentifikasi apakah ada masalah dengan logika evaluasi AWS Lambda fungsi Anda. AWS Config

Contoh

1. Anda membuat aturan khusus yang mengevaluasi apakah pengguna IAM Anda memiliki kunci akses aktif.
2. AWS Config mengevaluasi sumber daya Anda terhadap aturan khusus Anda.
3. Pengguna IAM yang tidak memiliki kunci akses aktif ada di akun Anda. Aturan Anda tidak menandai sumber daya ini dengan benar sebagai NON_COMPLIANT.
4. Anda memperbaiki aturan dan memulai evaluasi lagi.
5. Karena Anda memperbaiki aturan, aturan mengevaluasi sumber daya Anda dengan benar, dan menandai sumber daya pengguna IAM sebagai NON_COMPLIANT.

Ketika Anda menambahkan aturan ke akun Anda, Anda dapat menentukan kapan dalam proses pembuatan dan manajemen sumber daya yang AWS Config ingin Anda evaluasi sumber daya Anda. Proses pembuatan dan manajemen sumber daya dikenal sebagai penyediaan sumber daya. Anda memilih mode evaluasi untuk menentukan kapan dalam proses ini Anda AWS Config ingin mengevaluasi sumber daya Anda.

Tergantung pada aturan, AWS Config dapat mengevaluasi konfigurasi sumber daya Anda sebelum sumber daya telah digunakan, setelah sumber daya telah digunakan, atau keduanya. Mengevaluasi sumber daya sebelum digunakan adalah evaluasi proaktif. Mengevaluasi sumber daya setelah dikerahkan adalah evaluasi detektif.

Modus proaktif

Gunakan evaluasi proaktif untuk mengevaluasi sumber daya sebelum digunakan. Ini memungkinkan Anda untuk mengevaluasi apakah satu set properti sumber daya, jika digunakan untuk mendefinisikan AWS sumber daya, akan COMPLIANT atau NON_COMPLIANT mengingat seperangkat aturan proaktif yang Anda miliki di akun Anda di Wilayah Anda.

Skema tipe Resource menyatakan properti sumber daya. Anda dapat menemukan skema jenis sumber daya di "ekstensi AWS publik" di dalam AWS CloudFormation registri atau dengan CLI commmand berikut:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

Untuk informasi selengkapnya, lihat Mengelola ekstensi melalui referensi AWS CloudFormation registri dan AWS sumber daya serta tipe properti di Panduan AWS CloudFormation Pengguna.

> **Note**
>
> Aturan proaktif tidak memulihkan sumber daya yang ditandai sebagai NON_COMPLIANT atau mencegahnya diterapkan.

Mengevaluasi Sumber Daya Anda

Untuk mengaktifkan evaluasi proaktif

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Di AWS Management Console menu, verifikasi bahwa pemilih Wilayah diatur ke Wilayah yang mendukung AWS Config aturan. Untuk daftar AWS Wilayah yang didukung, lihat AWS Config Wilayah dan Titik Akhir di. Referensi Umum Amazon Web Services
3. Di navigasi kiri, pilih Aturan. Untuk daftar aturan terkelola yang mendukung evaluasi proaktif, lihat Daftar Aturan AWS Config Terkelola menurut Mode Evaluasi.
4. Pilih aturan, lalu pilih Edit aturan untuk aturan yang ingin Anda perbarui.

5. Untuk mode Evaluasi, pilih Aktifkan evaluasi proaktif untuk memungkinkan Anda menjalankan evaluasi pada pengaturan konfigurasi sumber daya Anda sebelum diterapkan.
6. Pilih Simpan.

> **Note**
>
> Anda juga dapat mengaktifkan evaluasi proaktif menggunakan `put-config-rule`perintah dan mengaktifkan `PROACTIVE` untuk `EvaluationModes` atau menggunakan PutConfigRuletindakan dan mengaktifkan `PROACTIVE` untuk. `EvaluationModes`

Setelah mengaktifkan evaluasi proaktif, Anda dapat menggunakan StartResourceEvaluationAPI dan GetResourceEvaluationSummaryAPI untuk memeriksa apakah sumber daya yang Anda tentukan dalam perintah ini akan ditandai sebagai NON_COMPLIANT oleh aturan proaktif di akun Anda di Wilayah Anda.

Misalnya, mulai dengan StartResourceEvaluation API:

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

Anda harus menerima `ResourceEvaluationId` dalam output:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Kemudian, gunakan `ResourceEvaluationId` dengan GetResourceEvaluationSummary API untuk memeriksa hasil evaluasi:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

Anda harus menerima output yang mirip dengan yang berikut ini:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

Untuk melihat informasi tambahan tentang hasil evaluasi, seperti aturan yang menandai sumber daya sebagai NON_COMPLIANT, gunakan API. GetComplianceDetailsByResource

Mode Detektif

Gunakan evaluasi detektif untuk mengevaluasi sumber daya yang telah digunakan. Ini memungkinkan Anda untuk mengevaluasi pengaturan konfigurasi sumber daya yang ada.

Mengevaluasi Sumber Daya Anda (Konsol)

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Di AWS Management Console menu, periksa apakah pemilih wilayah diatur ke Wilayah yang mendukung AWS Config aturan. Untuk daftar wilayah yang didukung, lihat AWS Config Wilayah dan Titik Akhir di. Referensi Umum Amazon Web Services
3. Di panel navigasi, pilih Aturan. Halaman Aturan menunjukkan nama, tindakan remediasi terkait, dan status kepatuhan setiap aturan.
4. Pilih aturan dari tabel.
5. Dari daftar dropdown Tindakan, pilih Evaluasi ulang.
6. AWS Config mulai mengevaluasi sumber daya terhadap aturan Anda.

> **Note**
>
> Anda dapat mengevaluasi kembali aturan satu kali setiap menit. Anda harus menunggu AWS Config untuk menyelesaikan evaluasi untuk aturan Anda sebelum Anda memulai evaluasi lain. Anda tidak dapat menjalankan evaluasi jika pada saat yang sama aturan sedang diperbarui atau jika aturan sedang dihapus.

Mengevaluasi Sumber Daya Anda (CLI)

- Gunakan start-config-rules-evaluation perintah:

```
$ aws configservice start-config-rules-evaluation --config-rule-
names ConfigRuleName
```

AWS Config mulai mengevaluasi konfigurasi sumber daya yang direkam terhadap aturan Anda. Anda juga dapat menentukan beberapa aturan dalam permintaan Anda:

```
$ aws configservice start-config-rules-evaluation --config-rule-
names ConfigRuleName1 ConfigRuleName2 ConfigRuleName3
```

Mengevaluasi Sumber Daya Anda (API)

Gunakan StartConfigRulesEvaluationtindakan.

Menghapus Hasil Evaluasi dari Aturan AWS Config

Setelah AWS Config mengevaluasi aturan Anda, Anda dapat melihat hasil evaluasi di halaman Aturan atau halaman detail Aturan untuk aturan tersebut. Jika hasil evaluasi salah atau jika Anda ingin mengevaluasi lagi, Anda dapat menghapus hasil evaluasi saat ini untuk aturan tersebut. Misalnya, jika aturan Anda salah mengevaluasi sumber daya Anda atau sumber daya yang baru saja dihapus dari akun, Anda dapat menghapus hasil evaluasi dan kemudian menjalankan evaluasi baru.

Deleting Evaluation Results (Console)

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.

2. Di AWS Management Console menu, verifikasi bahwa pemilih Wilayah diatur ke AWS Wilayah yang mendukung AWS Config aturan. Untuk daftar Wilayah yang didukung, lihat AWS Config Wilayah dan Titik Akhir di. Referensi Umum Amazon Web Services
3. Di panel navigasi, pilih Aturan. Halaman Aturan menunjukkan nama, tindakan remediasi terkait, dan status kepatuhan setiap aturan.
4. Pilih aturan dari tabel.
5. Dari daftar dropdown Tindakan, pilih Hapus hasil.
6. Saat diminta, ketik Hapus (entri ini peka huruf besar/kecil), lalu pilih Hapus. Setelah Anda menghapus evaluasi, Anda tidak dapat mengambilnya.
7. Setelah hasil evaluasi dihapus, Anda dapat memulai evaluasi baru secara manual.

Deleting Evaluation Results (CLI)

- Gunakan perintah delete-evaluation-results.

```
$ aws configservice delete-evaluation-results --config-rule-name ConfigRuleName
```

  AWS Config menghapus hasil evaluasi untuk aturan tersebut.

Deleting Evaluation Results (API)

Gunakan DeleteEvaluationResultstindakan.

Pemecahan masalah untuk aturan AWS Config

Periksa masalah berikut untuk memecahkan masalah jika Anda tidak dapat menghapus AWS Config aturan atau menerima kesalahan serupa dengan berikut: “Kesalahan telah terjadi dengan.” AWS Config

Entitas AWS Identity and Access Management (IAM) memiliki izin untuk API DeleteConfigRule

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi pilih Pengguna atau Peran.
3. Pilih pengguna atau peran yang Anda gunakan untuk menghapus AWS Config aturan, dan memperluas kebijakan Izin.

4. Di tab Izin, pilih JSON.
5. Di panel pratinjau JSON, konfirmasikan bahwa kebijakan IAM mengizinkan izin untuk API. DeleteConfigRule

Batas izin entitas IAM memungkinkan API DeleteConfigRule

Jika entitas IAM memiliki batas izin, pastikan bahwa entitas IAM mengizinkan izin untuk API. DeleteConfigRule

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi pilih Pengguna atau Peran.
3. Pilih pengguna atau peran yang Anda gunakan untuk menghapus AWS Config aturan, memperluas batas Izin, lalu pilih JSON.
4. Di panel pratinjau JSON, konfirmasikan bahwa kebijakan IAM mengizinkan izin untuk API. DeleteConfigRule

> **Warning**
>
> Pengguna IAM memiliki kredensi jangka panjang, yang menghadirkan risiko keamanan. Untuk membantu mengurangi risiko ini, kami menyarankan agar Anda memberikan pengguna ini hanya izin yang mereka perlukan untuk melakukan tugas dan menghapus pengguna ini ketika mereka tidak lagi diperlukan.

Kebijakan kontrol layanan (SCP) memungkinkan API DeleteConfigRule

1. Buka AWS Organizations konsol saat https://console.aws.amazon.com/organizations/ menggunakan akun manajemen untuk organisasi.
2. Di Nama akun, pilih Akun AWS.
3. Dalam Kebijakan, perluas kebijakan kontrol Layanan dan catat kebijakan SCP yang dilampirkan.
4. Di bagian atas halaman, pilih Kebijakan.
5. Pilih kebijakan, lalu pilih Lihat detail.
6. Di panel pratinjau JSON, konfirmasikan bahwa kebijakan mengizinkan API. DeleteConfigRule

Aturannya bukan aturan terkait layanan

Saat Anda mengaktifkan standar keamanan, AWS Security Hub buat aturan terkait layanan untuk Anda. Anda tidak dapat menghapus aturan terkait layanan ini menggunakan AWS Config, dan tombol hapus berwarna abu-abu. Untuk menghapus aturan terkait layanan, lihat Menonaktifkan standar keamanan di Panduan Pengguna Security Hub.

Tidak ada tindakan remediasi yang sedang berlangsung

Anda tidak dapat menghapus AWS Config aturan yang memiliki tindakan remediasi yang sedang berlangsung. Ikuti langkah-langkah untuk menghapus tindakan remediasi yang terkait dengan aturan tersebut. Kemudian, coba hapus aturan lagi.

> **Important**
>
> Hanya hapus tindakan remediasi yang berada dalam status gagal atau berhasil.

Paket Kesesuaian untuk AWS Config

Paket kesesuaian adalah kumpulan AWS Config aturan dan tindakan remediasi yang dapat dengan mudah digunakan sebagai entitas tunggal dalam akun dan Wilayah atau di seluruh organisasi di. AWS Organizations

Paket kesesuaian dibuat dengan membuat template YAMM yang berisi daftar aturan AWS Config terkelola atau kustom dan tindakan remediasi. Anda juga dapat menggunakan AWS Systems Manager dokumen (dokumen SSM) untuk menyimpan templat paket kesesuaian Anda AWS dan langsung menyebarkan paket kesesuaian menggunakan nama dokumen SSM. Anda dapat menerapkan template dengan menggunakan AWS Config konsol atau file. AWS CLI

Untuk memulai dengan cepat dan mengevaluasi AWS lingkungan Anda, gunakan salah satu contoh templat paket kesesuaian. Anda juga dapat membuat paket kesesuaian file YAMM dari awal berdasarkan Paket Kesesuaian Kustom.

Topik

- Melihat Data Kepatuhan di Dasbor Paket Kesesuaian untuk AWS Config
- Prasyarat untuk Paket Kesesuaian untuk AWS Config
- Support Wilayah
- AWS Config Memproses Pemeriksaan Dalam Paket Kesesuaian untuk AWS Config
- Templat Contoh Paket Kesesuaian untuk AWS Config
- Membuat template untuk Paket Kesesuaian Kustom untuk AWS Config
- Menyebarkan Paket Kesesuaian untuk AWS Config
- Mengedit Paket Kesesuaian untuk AWS Config
- Menghapus Paket Kesesuaian untuk AWS Config
- Melihat Detail dan Informasi Kepatuhan untuk Paket Kesesuaian Anda AWS Config
- Melihat Timeline Riwayat Kepatuhan untuk Paket Kesesuaian untuk AWS Config
- Menanyakan Riwayat Kepatuhan untuk Paket Kesesuaian untuk AWS Config
- Mengelola Paket Kesesuaian untuk Semua Akun AWS Config di Organisasi Anda
- Pemecahan Masalah untuk Paket Kesesuaian untuk AWS Config

Melihat Data Kepatuhan di Dasbor Paket Kesesuaian untuk AWS Config

Halaman utama untuk Conformance Packs menampilkan semua paket kesesuaian yang saat ini Anda miliki di. Akun AWS Halaman ini juga berisi nama, status penerapan, dan skor kepatuhan dari setiap paket kesesuaian. Skor kepatuhan adalah persentase dari jumlah kombinasi aturan-sumber daya yang sesuai dalam paket kesesuaian dibandingkan dengan jumlah total kemungkinan kombinasi aturan-sumber daya dalam paket kesesuaian.

Anda dapat menggunakan dasbor ini untuk memahami tingkat kepatuhan paket kesesuaian Anda dan menggunakan skor kepatuhan untuk melacak kemajuan remediasi, melakukan perbandingan di berbagai rangkaian persyaratan, dan melihat dampak perubahan atau penerapan tertentu terhadap paket kesesuaian.

Menavigasi Halaman Utama Paket Kesesuaian

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Arahkan ke halaman paket Kesesuaian. Tinjau paket kesesuaian Anda dan skor kepatuhannya. Anda juga dapat melakukan hal berikut:
   - Untuk menambahkan dan mengonfigurasi paket kesesuaian baru, pilih Deploy conformance pack.
   - Untuk menghapus paket kesesuaian dan datanya, mengubah pengaturan konfigurasi, atau melihat detail tambahan, seperti lokasi pengiriman atau parameter, pilih paket kesesuaian dan pilih Tindakan.

     > **Note**
     >
     > Anda tidak dapat mengedit paket kesesuaian yang diterapkan. Anda dapat memodifikasi pilihan lain kapan saja dengan memilih nama paket kesesuaian dan Edit di dropdown Tindakan.

   - Untuk melihat riwayat perubahan status kepatuhan, pilih paket kesesuaian dan pilih Timeline paket kesesuaian. Untuk informasi selengkapnya, lihat Melihat Garis Waktu Riwayat Kepatuhan untuk Paket Kesesuaian.

- Untuk melihat status penerapan, skor kepatuhan, garis waktu skor kepatuhan, dan aturan untuk paket kesesuaian dalam tampilan mendetail, pilih paket kesesuaian dan pilih Lihat.

Prasyarat untuk Paket Kesesuaian untuk AWS Config

Sebelum Anda menerapkan paket kesesuaian Anda, aktifkan perekaman. AWS Config

Topik

- Langkah 1: Mulai AWS Config Merekam (Diperlukan untuk semua paket kesesuaian)
- Langkah 2: Prasyarat Tambahan berdasarkan Jenis Paket Kesesuaian

Langkah 1: Mulai AWS Config Merekam (Diperlukan untuk semua paket kesesuaian)

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Pilih Pengaturan di panel navigasi.
3. Untuk mulai merekam, di bawah Perekaman dinonaktifkan, pilih Aktifkan. Saat diminta, pilih Lanjutkan.

Langkah 2: Prasyarat Tambahan berdasarkan Jenis Paket Kesesuaian

A. Prasyarat untuk Menggunakan Paket Kesesuaian Dengan Remediasi

Sebelum menerapkan paket kesesuaian menggunakan template sampel dengan remediasi, Anda harus membuat sumber daya yang sesuai seperti otomatisasi mengambil peran dan sumber AWS daya lain berdasarkan target remediasi Anda.

Jika Anda memiliki peran otomatisasi yang ada yang Anda gunakan untuk remediasi menggunakan dokumen SSM, Anda dapat langsung memberikan ARN peran itu. Jika Anda memiliki sumber daya apa pun, Anda dapat menyediakannya di template.

> **Note**
>
> Saat menerapkan paket kesesuaian dengan remediasi ke organisasi, ID akun manajemen organisasi harus ditentukan. Jika tidak, selama penyebaran paket kesesuaian organisasi AWS Config menggantikan ID akun manajemen dengan ID akun anggota secara otomatis.

AWS Config tidak mendukung fungsi AWS CloudFormation intrinsik untuk peran eksekusi otomatisasi atau. `ConfigRuleName` Anda harus memberikan ARN yang tepat dari peran sebagai string, dan Anda harus menggunakan nama aturan lengkap tanpa fungsi intrinsik.

Untuk informasi lebih lanjut tentang cara melewati ARN yang tepat, lihat. Templat Contoh Paket Kesesuaian untuk AWS Config Saat menggunakan contoh templat, perbarui ID Akun dan ID akun manajemen Anda untuk organisasi.

B. Prasyarat untuk Menggunakan Paket Kesesuaian Dengan Satu atau Lebih Aturan Kustom AWS Config

Sebelum menerapkan paket kesesuaian dengan satu atau beberapa AWS Config aturan khusus, buat sumber daya yang sesuai seperti AWS Lambda fungsi dan peran eksekusi yang sesuai.

Jika Anda memiliki AWS Config aturan kustom yang ada, Anda dapat langsung menyediakan AWS Lambda fungsi `ARN` of untuk membuat instance lain dari aturan kustom tersebut sebagai bagian dari paket.

Jika Anda tidak memiliki AWS Config aturan kustom yang ada, Anda dapat membuat AWS Lambda fungsi dan menggunakan ARN dari fungsi Lambda. Untuk informasi selengkapnya, lihat AWS Config Aturan Kustom.

Jika AWS Lambda fungsi Anda hadir dalam yang berbeda Akun AWS, Anda dapat membuat AWS Config aturan dengan otorisasi AWS Lambda fungsi lintas akun yang sesuai. Untuk informasi selengkapnya, lihat Cara Mengelola AWS Config Aturan Secara Terpusat di Beberapa posting Akun AWS blog.

Same account bucket policy

> AWS Config Agar dapat menyimpan artefak paket kesesuaian, Anda harus menyediakan bucket Amazon S3 dan menambahkan izin berikut. Untuk informasi selengkapnya tentang penamaan bucket, lihat Aturan penamaan bucket.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigConformsBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::AccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::delivery-bucket-name"
    },
    {
      "Sid": "AWSConfigConformsBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::AccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::delivery-bucket-name/[optional] prefix/
AWSLogs/AccountId/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    }
  ]
}
```

Cross-account bucket policy

AWS Config Agar dapat menyimpan artefak paket kesesuaian, Anda harus menyediakan bucket Amazon S3 dan menambahkan izin berikut. Untuk informasi selengkapnya tentang penamaan bucket, lihat Aturan penamaan bucket.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigConformsBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::SourceAccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms",
            "PutConformancePack API caller user principal like
 arn:aws:iam::SourceAccountId:user/userName "
        ]
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name"
    },
    {
      "Sid": "AWSConfigConformsBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::SourceAccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/
[optional] prefix/AWSLogs/AccountID/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    },
```

```
    {
      "Sid": " AWSConfigConformsBucketReadAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::SourceAccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/
[optional] prefix/AWSLogs/AccountID/Config/*"
    }
  ]
}
```

> **Note**
>
> Saat menerapkan paket kesesuaian lintas akun, nama bucket Amazon S3 pengiriman harus dimulai dengan. `awsconfigconforms`

C. Prasyarat untuk Paket Kesesuaian Organisasi

Tentukan peran eksekusi otomatisasi ARN untuk remediasi tersebut dalam template jika template input memiliki konfigurasi autoremediasi. Pastikan peran dengan nama yang ditentukan ada di semua akun (manajemen dan anggota) organisasi. Anda harus membuat peran ini di semua akun sebelum meneleponPutOrganizationConformancePack. Anda dapat membuat peran ini secara manual atau menggunakan AWS CloudFormation stack-set untuk membuat peran ini di setiap akun.

Jika template Anda menggunakan fungsi AWS CloudFormation intrinsik `Fn::ImportValue` untuk mengimpor variabel tertentu, maka variabel tersebut harus didefinisikan sebagai `Export Value` di semua akun anggota organisasi tersebut.

Untuk AWS Config aturan kustom, lihat Cara Mengelola AWS Config Aturan Secara Terpusat di Beberapa Akun AWS blog untuk mengatur izin yang tepat.

Kebijakan bucket organisasi:

AWS Config Agar dapat menyimpan artefak paket kesesuaian, Anda harus menyediakan bucket Amazon S3 dan menambahkan izin berikut. Untuk informasi selengkapnya tentang penamaan bucket, lihat Aturan penamaan bucket.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                 "s3:GetObject",
                 "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "customer_org_id"
                },
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::*:role/aws-service-role/
config-conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                }
            }
        },
        {
            "Sid": "AllowGetBucketAcl",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "customer_org_id"
                },
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::*:role/aws-service-role/
config-conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                }
```

```
            }
        }
    ]
}
```

> **Note**
>
> Saat menerapkan paket kesesuaian ke organisasi, nama bucket Amazon S3 pengiriman harus dimulai dengan. `awsconfigconforms`

Support Wilayah

Paket kesesuaian didukung di Wilayah berikut.

Nama Wilayah	Wilayah	Titik Akhir	Protokol
AS Timur (Ohio)	us–east-2	config.us-east-2.amazonaws.com	HTTPS
AS Timur (Virginia Utara)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
AS Barat (Californ ia Utara)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
AS Barat (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
Afrika (Cape Town)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asia Pasifik	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
(Hong Kong)			
Asia Pasifik (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asia Pasifik (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asia Pasifik (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia Pasifik (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pasifik (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia Pasifik (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia Pasifik (Singapura)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Asia Pasifik (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Kanada (Pusat)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Kanada Barat (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Eropa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Eropa (Irlandia)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Eropa (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Eropa (Milan)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Eropa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Eropa (Spanyol)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Eropa (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Eropa (Zürich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Timur Tengah (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Timur Tengah (UAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
Amerika Selatan (Sao Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (AS-Timur)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (AS-Barat)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Menerapkan paket kesesuaian di seluruh akun anggota di AWS Organisasi didukung di Wilayah berikut.

Nama Wilayah	Wilayah	Titik Akhir	Protokol
AS Timur (Ohio)	us–east-2	config.us-east-2.amazonaws.com	HTTPS
AS Timur (Virginia Utara)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
AS Barat (California Utara)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
AS Barat (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
Afrika (Cape Town)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asia Pasifik (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asia Pasifik (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asia Pasifik (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asia Pasifik	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
(Melbourne)			
Asia Pasifik (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pasifik (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia Pasifik (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia Pasifik (Singapura)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pasifik (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Kanada (Pusat)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Kanada Barat (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Eropa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Eropa (Irlandia)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Eropa (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Eropa (Milan)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Eropa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Eropa (Spanyol)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Eropa (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Eropa (Zürich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Timur Tengah (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Timur Tengah (UAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Amerika Selatan (Sao Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (AS-Timur)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (AS-Barat)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

AWS Config Memproses Pemeriksaan Dalam Paket Kesesuaian untuk AWS Config

Pemeriksaan proses adalah jenis AWS Config aturan yang memungkinkan Anda melacak tugas eksternal dan internal Anda yang memerlukan verifikasi sebagai bagian dari paket kesesuaian. Pemeriksaan ini dapat ditambahkan ke paket kesesuaian yang ada atau paket kesesuaian baru. Anda dapat melacak semua kepatuhan yang mencakup AWS Config urasi dan pemeriksaan manual di satu lokasi.

Dengan pemeriksaan proses, Anda dapat membuat daftar kepatuhan persyaratan dan tindakan di satu lokasi. Pemeriksaan proses ini membantu meningkatkan cakupan paket kesesuaian berbasis rezim kepatuhan. Anda dapat memperluas paket kesesuaian lebih lanjut dengan menambahkan pemeriksaan proses baru yang melacak proses dan tindakan yang memerlukan verifikasi dan pelacakan manual. Hal ini memungkinkan paket kesesuaian untuk menjadi template yang memberikan rincian tentang AWS Config urasi dan proses manual untuk rezim kepatuhan.

Anda dapat melacak dan mengelola kepatuhan proses yang tidak terkait dengan perubahan konfigurasi sumber daya dalam paket kesesuaian sebagai pemeriksaan proses. Misalnya, Anda dapat menambahkan pemeriksaan proses untuk melacak persyaratan kepatuhan PCI-DSS untuk

menyimpan cadangan media di lokasi di luar lokasi. Anda akan mengevaluasi kepatuhan ini secara manual sesuai dengan pedoman PCI-DSS, atau sesuai dengan panduan organisasi Anda.

Ketersediaan wilayah: Pemeriksaan proses dengan paket kesesuaian tersedia di semua Wilayah AWS tempat paket AWS Config kesesuaian tersedia. Untuk informasi selengkapnya, lihat Support Wilayah.

Topik

- Contoh Template Paket Kesesuaian untuk Membuat Pemeriksaan Proses
- Sertakan Pemeriksaan Proses Dalam Paket Kesesuaian
- Ubah Status Kepatuhan Pemeriksaan Proses
- Lihat dan Edit Pemeriksaan Proses (Konsol)

Contoh Template Paket Kesesuaian untuk Membuat Pemeriksaan Proses

```
################################################################################
#
#  Conformance Pack template for process check
#
################################################################################
Resources:
  AWSConfigProcessCheck:
    Properties:
      ConfigRuleName: RuleName
      Description: Description of Rule
      Source:
        Owner: AWS
        SourceIdentifier: AWS_CONFIG_PROCESS_CHECK
    Type: AWS::Config::ConfigRule
```

Lihat dua contoh template, Praktik Terbaik Operasional untuk Tolok Ukur AWS Yayasan CIS v1.4 Level 1 template dan Praktik Terbaik Operasional untuk Tolok Ukur AWS Yayasan CIS v1.4 Level 2 template.

Sertakan Pemeriksaan Proses Dalam Paket Kesesuaian

1. Tambahkan pemeriksaan proses di template paket kesesuaian. Lihat Contoh Template Paket Kesesuaian untuk Membuat Pemeriksaan Proses.

```
Resources:
  ConfigEnabledAllRegions:
    Properties:
      ConfigRuleName: Config-Enabled-All-Regions
      Description: Ensure AWS Config is enabled in all Regions.
      Source:
        Owner: AWS
        SourceIdentifier: AWS_CONFIG_PROCESS_CHECK
    Type: AWS::Config::ConfigRule
```

2. Masukkan nama untuk pemeriksaan proses.
3. Masukkan deskripsi untuk pemeriksaan proses.
4. Menyebarkan paket kesesuaian. Untuk informasi selengkapnya, lihat Menyebarkan Paket Kesesuaian untuk AWS Config.

Ubah Status Kepatuhan Pemeriksaan Proses

Anda dapat mengubah status kepatuhan pemeriksaan proses menggunakan AWS Config konsol, AWS CLI, dan APIs.

Change Compliance Status for Process Checks (Console)

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Arahkan ke halaman AWS Config Aturan.
3. Pilih nama pemeriksaan proses yang Anda tentukan dalam template bersama dengan pengenal dalam paket kesesuaian.

   > **Note**
   >
   > Semua pemeriksaan proses dari paket kesesuaian yang sama memiliki akhiran yang sama.

4. Pada halaman Rincian aturan, Anda tidak dapat mengedit aturan tetapi Anda dapat mengedit kepatuhan aturan. Di bagian Kepatuhan manual, pilih Edit kepatuhan.
5. Pilih kepatuhan yang sesuai dari daftar dropdown.
6. (Opsional) Masukkan deskripsi untuk status kepatuhan.

7. Pilih Simpan.

Change the Compliance Status for Process Checks (AWS CLI)

Anda dapat memperbarui kepatuhan pemeriksaan proses dalam paket kesesuaian menggunakan (). AWS Command Line Interface AWS CLI

Untuk menginstal AWS CLI pada mesin lokal Anda, lihat Menginstal AWS CLI di Panduan AWS CLI Pengguna.

Jika perlu, ketik `AWS Config ure` untuk mengkonfigurasi AWS CLI untuk menggunakan AWS Wilayah di mana paket AWS Config kesesuaian tersedia.

1. Buka jendela command prompt atau terminal.
2. Masukkan perintah berikut untuk memperbarui kepatuhan pemeriksaan proses di `ComplianceResourceId` mana Anda`Account ID`, dan sertakan nama aturan Anda.

```
aws configservice put-external-evaluation --config-rule-
name process-check-rule-name  --external-evaluation
 ComplianceResourceType=AWS::::Account,ComplianceResourceId=Account
 ID,ComplianceType=NON_COMPLIANT,OrderingTimestamp=2020-12-17T00:10:00.000Z
```

3. Tekan Enter untuk menjalankan perintah.

Change the Compliance Status for Process Checks (API)

Setelah penerapan selesai, untuk memperbarui evaluasi dan kepatuhan pemeriksaan proses, gunakan API. `PutExternalEvaluation` Untuk informasi selengkapnya, lihat PutExternalEvaluation.

Lihat dan Edit Pemeriksaan Proses (Konsol)

Anda dapat melihat pemeriksaan proses hanya setelah status kepatuhan ditambahkan ke pemeriksaan proses. Pilih paket kesesuaian khusus untuk melihat semua pemeriksaan proses dalam paket kesesuaian itu. Di sini Anda dapat melihat daftar pemeriksaan proses yang dalam status sesuai dan tidak patuh.

Karena ini adalah aturan terkait layanan, Anda tidak dapat mengedit pemeriksaan proses melalui halaman Rincian aturan.

> **Note**
>
> Namun, Anda dapat memperbarui kepatuhan pemeriksaan proses dengan memilih Edit Kepatuhan dan memilih nilai yang sesuai dari Compliant, noncompliant atau tidak berlaku.

Anda dapat mengedit atau menghapus pemeriksaan proses dari paket kesesuaian tempat Anda menambahkan pemeriksaan proses.

Templat Contoh Paket Kesesuaian untuk AWS Config

Berikut adalah template YAMAL paket kesesuaian yang Anda lihat di konsol. AWS Config Dalam setiap template paket kesesuaian, Anda dapat menggunakan satu atau beberapa AWS Config aturan dan tindakan remediasi. AWS Config Aturan yang tercantum dalam paket kesesuaian dapat AWS Config dikelola aturan dan/atau AWS Config aturan khusus. Anda dapat mengunduh semua templat paket kesesuaian dari. GitHub

> **Important**
>
> Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum untuk membantu Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config AWS Templat sampel paket kesesuaian dimaksudkan untuk membantu Anda membuat paket kesesuaian Anda sendiri dengan aturan yang berbeda atau tambahan, parameter masukan, dan tindakan remediasi yang sesuai dengan lingkungan Anda. Contoh template, termasuk yang terkait dengan standar kepatuhan dan tolok ukur industri, tidak dirancang untuk memastikan kepatuhan Anda terhadap standar tata kelola tertentu. Mereka tidak dapat menggantikan upaya internal Anda atau menjamin bahwa Anda akan lulus penilaian kepatuhan.

> **Note**
>
> Anda disarankan untuk meninjau aturan yang tersedia di wilayah tempat Anda menerapkan paket kesesuaian (Daftar Aturan AWS Config Terkelola menurut Ketersediaan Wilayah) dan mengubah templat untuk aturan yang belum tersedia di wilayah tersebut sebelum menerapkan.

Topik

- AWS Paket Kesesuaian Pagar Pembatas Detektif Menara Kontrol
- Praktik Terbaik Operasional untuk Beban Kerja Material ABS CCIG 2.0
- Praktik Terbaik Operasional untuk Beban Kerja Standar ABS CCIG 2.0
- Praktik Terbaik Operasional untuk ACSC Essential 8
- Praktik Terbaik Operasional untuk ACSC ISM
- Praktik Terbaik Operasional untuk AI dan ML
- Praktik Terbaik Operasional untuk Amazon API Gateway
- Praktik Terbaik Operasional untuk Amazon CloudWatch
- Praktik Terbaik Operasional untuk Amazon DynamoDB
- Praktik Terbaik Operasional untuk Amazon S3
- Praktik Terbaik Operasional untuk APRA CPG 234
- Praktik Terbaik Operasional untuk Manajemen Aset
- Praktik Terbaik Operasional untuk AWS Backup
- Praktik Terbaik Operasional untuk Manajemen AWS Identitas Dan Akses
- Praktik Terbaik Operasional untuk Pilar Keandalan AWS Kerangka Well-Architected
- Praktik Terbaik Operasional untuk Pilar Keamanan AWS Kerangka Well-Architected
- Praktik Terbaik Operasional untuk BCP dan DR
- Praktik Terbaik Operasional untuk BNM T RMi
- Praktik Terbaik Operasional untuk Profil Kontrol Cloud Sedang Pusat Keamanan Siber Kanada (CCCS)
- Praktik Terbaik Operasional untuk Tolok Ukur AWS Yayasan CIS v1.4 Level 1
- Praktik Terbaik Operasional untuk Tolok Ukur AWS Yayasan CIS v1.4 Level 2
- Praktik Terbaik Operasional untuk Kontrol Keamanan Kritis CIS v8 IG1
- Praktik Terbaik Operasional untuk Kontrol Keamanan Kritis CIS v8 IG2
- Praktik Terbaik Operasional untuk Kontrol Keamanan Kritis CIS v8 IG3
- Praktik Terbaik Operasional untuk CIS Top 20
- Praktik Terbaik Operasional untuk CISA Cyber Essentials
- Praktik Terbaik Operasional untuk Layanan Informasi Peradilan Pidana (CJIS)
- Praktik Terbaik Operasional untuk CMMC 2.0 Level 1
- Praktik Terbaik Operasional untuk CMMC 2.0 Level 2

- Praktik Terbaik Operasional untuk Layanan Komputasi
- Praktik Terbaik Operasional untuk Ketahanan Data
- Praktik Terbaik Operasional untuk Layanan Database
- Praktik Terbaik Operasional untuk Data Lakes dan Layanan Analytics
- Praktik Terbaik Operasional untuk DevOps
- Praktik Terbaik Operasional untuk EC2
- Praktik Terbaik Operasional untuk Enkripsi dan Manajemen Kunci
- Praktik Terbaik Operasional untuk Panduan Keamanan Siber ENISA untuk SMEs
- Praktik Terbaik Operasional untuk Esquema Nacional de Seguridad (ENS) Rendah
- Praktik Terbaik Operasional untuk Medium Esquema Nacional de Seguridad (ENS)
- Praktik Terbaik Operasional untuk Esquema Nacional de Seguridad (ENS) High
- Praktik Terbaik Operasional untuk FDA Judul 21 CFR Bagian 11
- Praktik Terbaik Operasional untuk FedRAMP (Rendah)
- Praktik Terbaik Operasional untuk FedRAMP (Sedang)
- Praktik Terbaik Operasional untuk FedRAMP (Bagian Tinggi 1)
- Praktik Terbaik Operasional untuk FedRAMP (Bagian Tinggi 2)
- Praktik Terbaik Operasional untuk FFIEC
- Praktik Terbaik Operasional untuk Katalog Kriteria Kepatuhan Komputasi Awan Jerman (C5)
- Praktik Terbaik Operasional untuk Gramm Leach Bliley Act (GLBA)
- Praktik Terbaik Operasional untuk GxP EU Annex 11
- Praktik Terbaik Operasional untuk Keamanan HIPAA
- Praktik Terbaik Operasional untuk IRS 1075
- Praktik Terbaik Operasional untuk K-ISMS
- Praktik Terbaik Operasional untuk Load Balancing
- Praktik Terbaik Operasional untuk Penebangan
- Praktik Terbaik Operasional untuk Layanan Manajemen dan Tata Kelola
- Praktik Terbaik Operasional untuk Pemberitahuan MAS 655
- Praktik Terbaik Operasional untuk MAS TRMG
- Praktik Terbaik Operasional untuk Pemantauan
- Praktik Terbaik Operasional untuk NBC TRMG

- Praktik Terbaik Operasional untuk NERC CIP BCSI
- Praktik Terbaik Operasional untuk Prinsip Keamanan Cloud NCSC
- Praktik Terbaik Operasional untuk Kerangka Penilaian Cyber NCSC
- Praktik Terbaik Operasional untuk Jaringan dan Layanan Pengiriman Konten
- Praktik Terbaik Operasional untuk NIST 800-53 rev 4
- Praktik Terbaik Operasional untuk NIST 800-53 rev 5
- Praktik Terbaik Operasional untuk NIST 800 171
- Praktik Terbaik Operasional untuk NIST 800 172
- Praktik Terbaik Operasional untuk NIST 800 181
- Praktik Terbaik Operasional untuk NIST 1800 25
- Praktik Terbaik Operasional untuk NIST CSF
- Praktik Terbaik Operasional untuk Kerangka Privasi NIST v1.0
- Praktik Terbaik Operasional untuk NYDFS 23
- Praktik Terbaik Operasional untuk NZISM 3.8
- Praktik Terbaik Operasional untuk PCI DSS 3.2.1
- Praktik Terbaik Operasional untuk PCI DSS 4.0 (Tidak termasuk jenis sumber daya global)
- Praktik Terbaik Operasional untuk PCI DSS 4.0 (Termasuk jenis sumber daya global)
- Praktik Terbaik Operasional untuk Sumber Daya yang Dapat Diakses Publik
- Praktik Terbaik Operasional untuk Kerangka Keamanan Cyber RBI untuk UCBs
- Praktik Terbaik Operasional untuk RBI MD-ITF
- Praktik Terbaik Operasional untuk Layanan Keamanan, Identitas, dan Kepatuhan
- Praktik Terbaik Operasional untuk Tanpa Server
- Praktik Terbaik Operasional untuk Layanan Penyimpanan
- Praktik Terbaik Operasional untuk SWIFT CSP
- Praktik Terbaik Keamanan untuk Amazon Elastic Container Service (Amazon ECS)
- Praktik Terbaik Keamanan untuk Amazon Elastic File System (Amazon EFS)
- Praktik Terbaik Keamanan untuk Amazon Elastic Kubernetes Service (Amazon EKS)
- Praktik Terbaik Keamanan untuk Amazon CloudFront
- Praktik Terbaik Keamanan untuk OpenSearch Layanan Amazon
- Praktik Terbaik Keamanan untuk Amazon Redshift

- Praktik Terbaik Keamanan untuk Amazon Relational Database Service (Amazon RDS)
- Praktik Terbaik Keamanan untuk AWS Auto Scaling
- Praktik Terbaik Keamanan untuk AWS CloudTrail
- Praktik Terbaik Keamanan untuk AWS CodeBuild
- Praktik Terbaik Keamanan untuk Amazon ECR
- Praktik Terbaik Keamanan untuk AWS Lambda
- Praktik Terbaik Keamanan untuk AWS Network Firewall
- Praktik Terbaik Keamanan untuk Amazon SageMaker AI
- Praktik Terbaik Keamanan untuk AWS Secrets Manager
- Praktik Terbaik Keamanan untuk AWS WAF
- Contoh Template dengan Tindakan Remediasi

AWS Paket Kesesuaian Pagar Pembatas Detektif Menara Kontrol

Paket kesesuaian ini berisi AWS Config aturan berdasarkan Control AWS Tower Detective Guardrails. Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template ini tersedia di GitHub: AWS Control Tower Detective Guardrails Conformance Pack.

Praktik Terbaik Operasional untuk Beban Kerja Material ABS CCIG 2.0

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini menyediakan contoh pemetaan antara ABS Cloud Computing Implementation Guide 2.0 - Beban Kerja Material dan aturan AWS Config terkelola. Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau beberapa kontrol Panduan Implementasi

Komputasi Awan ABS. Kontrol Panduan Implementasi Komputasi Awan ABS dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -2-material-beban kerja a-govern-the-cloud	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
bagian4 -2-material-beban kerja a-govern-the-cloud	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -2-beban kerja standar a-govern-the-cloud	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organ izations membantu memastika n bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabk an konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.
bagian4 -2-beban kerja standar a-govern-the-cloud	cloudtrail-s3-dataevents-di aktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
bagian4 -2-beban kerja standar a-govern-the-cloud	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktif an beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -2-beban kerja standar a-govern-the-cloud	cloudwatch-alarm-action-check	Amazon CloudWatch memperingatkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.
bagian4 -2-beban kerja standar a-govern-the-cloud	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -2-beban kerja standar a-govern-the-cloud	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.
bagian4 -2-beban kerja standar a-govern-the-cloud	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -2-beban kerja standar a-govern-the-cloud	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -3-material-beban kerja a-govern-the-cloud	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -3-material-beban kerja a-govern-the-cloud	lambda-concurrency-check	Aturan ini memastikan bahwa batas tinggi dan rendah konkurensi fungsi Lambda ditetapkan. Ini dapat membantu dalam menyusun dasar jumlah permintaan yang dilayani oleh fungsi Anda pada waktu tertentu.
bagian4 -3-beban kerja standar a-govern-the-cloud	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -3-beban kerja standar a-govern-the-cloud	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan , sesuai dengan standar organisasi Anda.
bagian4 -3-beban kerja standar a-govern-the-cloud	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirk an ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -3-beban kerja standar a-govern-the-cloud	terlampir eip	Aturan ini memastikan Elastic yang IPs dialokasi kan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan . Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.
bagian4 -3-beban kerja standar a-govern-the-cloud	vpc-network-acl-unused-periksa	Aturan ini memastikan bahwa daftar kontrol akses jaringan Amazon Virtual Private Cloud (VPC) sedang digunakan . Pemantauan untuk daftar kontrol akses jaringan yang tidak digunakan dapat membantu inventaris dan pengelolaan lingkungan Anda yang akurat.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribus i kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertah ankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi, pengembalian, dan pendelegasian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigurasi ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositori data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	ecs-containers-nonprivileged	Untuk membantu menerapkan prinsip hak istimewa paling rendah, definisi tugas Amazon Elastic Container Service (Amazon ECS) seharusnya tidak mengaktifkan hak istimewa yang ditinggikan. Ketika parameter ini benar, wadah diberikan hak istimewa yang ditinggikan pada instance wadah host (mirip dengan pengguna root).
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
bagian4 -the-cloud-2-beban kerja standar b-design-and-secure	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-2-beban kerja standar b-design-and-secure	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.
bagian4 -the-cloud-2-beban kerja standar b-design-and-secure	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapka n status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigura si aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-2-beban kerja standar b-design-and-secure	ec2- -periksa managedin stance-patch-compliance-sta tus	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
bagian4 -the-cloud-2-beban kerja standar b-design-and-secure	redshift-cluster-maintenanc esettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengatura n yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrad e. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00 -sat: 16:30), dan automated SnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-3-material-beban kerja b-design-and-secure	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.
bagian4 -the-cloud-3-material-beban kerja b-design-and-secure	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-3-material-beban kerja b-design-and-secure	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
bagian4 -the-cloud-3-material-beban kerja b-design-and-secure	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-3-material-beban kerja b-design-and-secure	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-3-material-beban kerja b-design-and-secure	rds-cluster-multi-az-diaktifkan	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-3-material-beban kerja b-design-and-secure	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.
bagian4 -the-cloud-3-standard-beban kerja b-design-and-secure	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-3-standard-beban kerja b-design-and-secure	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.
bagian4 -the-cloud-3-standard-beban kerja b-design-and-secure	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-3-standard-beban kerja b-design-and-secure	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.
bagian4 -the-cloud-3-standard-beban kerja b-design-and-secure	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-3-standard-beban kerja b-design-and-secure	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-3-standard-beban kerja b-design-and-secure	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-3-standard-beban kerja b-design-and-secure	rds-cluster-multi-az-diaktifkan	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-3-standard-beban kerja b-design-and-secure	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.
bagian4 -the-cloud-4-material-beban kerja b-design-and-secure	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-material-beban kerja b-design-and-secure	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindungi nya dari serangan berbahaya
bagian4 -the-cloud-4-material-beban kerja b-design-and-secure	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-material-beban kerja b-design-and-secure	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
bagian4 -the-cloud-4-material-beban kerja b-design-and-secure	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
bagian4 -the-cloud-4-material-beban kerja b-design-and-secure	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-material-beban kerja b-design-and-secure	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-material-beban kerja b-design-and-secure	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-material-beban kerja b-design-and-secure	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
bagian4 -the-cloud-4-material-beban kerja b-design-and-secure	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-material-beban kerja b-design-and-secure	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigurasi ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.
bagian4 -the-cloud-4-material-beban kerja b-design-and-secure	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-material-beban kerja b-design-and-secure	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
bagian4 -the-cloud-4-material-beban kerja b-design-and-secure	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-material-beban kerja b-design-and-secure	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
bagian4 -the-cloud-4-material-beban kerja b-design-and-secure	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-material-beban kerja b-design-and-secure	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -the-cloud-4-material-beban kerja b-design-and-secure	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-material-beban kerja b-design-and-secure	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
bagian4 -the-cloud-4-material-beban kerja b-design-and-secure	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-material-beban kerja b-design-and-secure	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-material-beban kerja b-design-and-secure	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan . Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.
bagian4 -the-cloud-4-material-beban kerja b-design-and-secure	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-material-beban kerja b-design-and-secure	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	api-gw-associated-with-waf	AWS WAF memungkin kan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindung inya dari serangan berbahaya
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribus i kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertah ankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabun gkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandun g tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkin kan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizink an tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi, pengembalian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedAc tionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabun gkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkin kan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurang i peluang bagi identitas untuk menerima atau mempertah ankan hak istimewa yang berlebihan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentif ikasi, Anda harus menonakti fkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkin kan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabk an akses tidak sah ke sumber daya VPC Amazon.
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	lambda-function-public-acce ss-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyarat an untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahk an lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearc h Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,338 9,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	sagemaker-notebook-no-direc t-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimpleme ntasikan untuk mencapai persyaratan ketahanan . Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-S ite VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	s3- -dilarang bucket-level-publi c-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
bagian4 -the-cloud-5-material-beban kerja b-design-and-secure	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.
bagian4 -the-cloud-5-material-beban kerja b-design-and-secure	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-5-material-beban kerja b-design-and-secure	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
bagian4 -the-cloud-5-material-beban kerja b-design-and-secure	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-5-material-beban kerja b-design-and-secure	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
bagian4 -the-cloud-5-beban kerja standar b-design-and-secure	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -the-cloud-5-beban kerja standar b-design-and-secure	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-5-beban kerja standar b-design-and-secure	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabun gkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandun g tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkin kan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-5-beban kerja standar b-design-and-secure	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizink an tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi, pengembalian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedAc tionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-5-beban kerja standar b-design-and-secure	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkin kan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
bagian4 -the-cloud-5-beban kerja standar b-design-and-secure	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindung i data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperluka n pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.
bagian4 -cloud-6-material-beban kerja b-design-and-secure	cmk-backing-key-rotation-di aktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-6-material-beban kerja b-design-and-secure	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-6-material-beban kerja b-design-and-secure	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizink an tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi, pengembalian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedAc tionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-6-material-beban kerja b-design-and-secure	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
bagian4 -cloud-6-material-beban kerja b-design-and-secure	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-6-material-beban kerja b-design-and-secure	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	alb-http-drop-invalid-Header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-6-beban kerja standar b-design-and-secure	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-6-beban kerja standar b-design-and-secure	ec2- ebs-encryption-by-default	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-6-beban kerja standar b-design-and-secure	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certifica te Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-6-beban kerja standar b-design-and-secure	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certifica te Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-6-beban kerja standar b-design-and-secure	rds-snapshot-encrypted	Pastikan enkripsi diaktifka n untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	rds-storage-encrypted	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-6-beban kerja standar b-design-and-secure	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-6-beban kerja standar b-design-and-secure	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-6-beban kerja standar b-design-and-secure	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-6-beban kerja standar b-design-and-secure	sns-encrypted-kms	Untuk membantu melindung i data saat istirahat, pastikan topik Amazon Simple Notificat ion Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifika t SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	redshift-cluster-kms-enabled	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-8-material-beban kerja b-design-and-secure	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.
bagian4 -cloud-8-material-beban kerja b-design-and-secure	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-8-material-beban kerja b-design-and-secure	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahk an lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
bagian4 -cloud-8-material-beban kerja b-design-and-secure	root-account-hardware-mfa-d iaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-8-material-beban kerja b-design-and-secure	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifka n untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
bagian4 -cloud-8-beban kerja standar b-design-and-secure	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaima na ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-8-beban kerja standar b-design-and-secure	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organ izations membantu memastika n bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabk an konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.
bagian4 -cloud-8-beban kerja standar b-design-and-secure	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktif an beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-8-beban kerja standar b-design-and-secure	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribus i kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertah ankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-8-beban kerja standar b-design-and-secure	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-8-beban kerja standar b-design-and-secure	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-8-beban kerja standar b-design-and-secure	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizink an tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi, pengembalian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedAc tionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-8-beban kerja standar b-design-and-secure	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-8-beban kerja standar b-design-and-secure	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -cloud-8-beban kerja standar b-design-and-secure	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
bagian4 -cloud-8-beban kerja standar b-design-and-secure	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-8-beban kerja standar b-design-and-secure	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.
bagian4 -cloud-8-beban kerja standar b-design-and-secure	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-8-beban kerja standar b-design-and-secure	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
bagian4 -cloud-8-beban kerja standar b-design-and-secure	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurang i peluang bagi identitas untuk menerima atau mempertah ankan hak istimewa yang berlebihan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-8-beban kerja standar b-design-and-secure	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentif ikasi, Anda harus menonakti fkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-8-beban kerja standar b-design-and-secure	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahk an lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
bagian4 -cloud-8-beban kerja standar b-design-and-secure	root-account-hardware-mfa-d iaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-8-beban kerja standar b-design-and-secure	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifka n untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
bagian4 -cloud-9-beban kerja material b-design-and-secure	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktif an beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-9-beban kerja material b-design-and-secure	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
bagian4 -cloud-9-beban kerja material b-design-and-secure	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-9-beban kerja material b-design-and-secure	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
bagian4 -cloud-9-beban kerja material b-design-and-secure	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahk an lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-9-beban kerja material b-design-and-secure	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
bagian4 -cloud-9-beban kerja material b-design-and-secure	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-9-beban kerja standar b-design-and-secure	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penol akan dengan merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilka n, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
bagian4 -the-cloud-9-beban kerja standar b-design-and-secure	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabun gkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-9-beban kerja standar b-design-and-secure	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-9-beban kerja standar b-design-and-secure	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
bagian4 -the-cloud-9-beban kerja standar b-design-and-secure	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-9-beban kerja standar b-design-and-secure	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.
bagian4 -the-cloud-9-beban kerja standar b-design-and-secure	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-9-beban kerja standar b-design-and-secure	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
bagian4 -the-cloud-9-beban kerja standar b-design-and-secure	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurang i peluang bagi identitas untuk menerima atau mempertah ankan hak istimewa yang berlebihan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-9-beban kerja standar b-design-and-secure	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentif ikasi, Anda harus menonakti fkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-9-beban kerja standar b-design-and-secure	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahk an lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
bagian4 -the-cloud-9-beban kerja standar b-design-and-secure	root-account-hardware-mfa-d iaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-9-beban kerja standar b-design-and-secure	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifka n untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
bagian4 -the-cloud-9-beban kerja standar b-design-and-secure	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-10-material -beban kerja b-design-and-secure	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
bagian4 -cloud-10-material -beban kerja b-design-and-secure	cloudwatch-alarm-action-check	Amazon CloudWatch memperingatkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-10-material -beban kerja b-design-and-secure	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
bagian4 -cloud-10-material -beban kerja b-design-and-secure	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.
bagian4 -cloud-10-material -beban kerja b-design-and-secure	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastika n instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-10-material -beban kerja b-design-and-secure	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
bagian4 -cloud-10-material -beban kerja b-design-and-secure	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-10-material -beban kerja b-design-and-secure	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -cloud-10-material -beban kerja b-design-and-secure	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.
bagian4 -cloud-10-material -beban kerja b-design-and-secure	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-10-material -beban kerja b-design-and-secure	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.
bagian4 -cloud-10-material -beban kerja b-design-and-secure	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-10-material -beban kerja b-design-and-secure	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.
bagian4 -cloud-10-material -beban kerja b-design-and-secure	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahk an lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
bagian4 -cloud-10-material -beban kerja b-design-and-secure	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-10-material -beban kerja b-design-and-secure	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearc h Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
bagian4 -cloud-10-material -beban kerja b-design-and-secure	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-10-material -beban kerja b-design-and-secure	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
bagian4 -cloud-10-material -beban kerja b-design-and-secure	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositori data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-10-material -beban kerja b-design-and-secure	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,338 9,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -cloud-10-material -beban kerja b-design-and-secure	root-account-hardware-mfa-d iaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-10-material -beban kerja b-design-and-secure	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-10-material -beban kerja b-design-and-secure	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -cloud-10-material -beban kerja b-design-and-secure	sagemaker-notebook-no-direc t-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-10-material -beban kerja b-design-and-secure	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspo s informasi tentang akun, sumber daya, dan proses internal Anda.
bagian4 -cloud-10-material -beban kerja b-design-and-secure	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-10-material -beban kerja b-design-and-secure	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-10-material -beban kerja b-design-and-secure	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimpleme ntasikan untuk mencapai persyaratan ketahanan . Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-S ite VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.
bagian4 -cloud-10-material -beban kerja b-design-and-secure	s3- -dilarang bucket-level-publi c-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-10-material -beban kerja b-design-and-secure	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
bagian4 -the-cloud-10-beba n kerja standar b-design-and-secure	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaima na ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigurasi ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
bagian4 -cloud-11-beban kerja material b-design-and-secure	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
bagian4 -cloud-11-beban kerja material b-design-and-secure	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-11-beban kerja material b-design-and-secure	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktif an beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.
bagian4 -cloud-11-beban kerja material b-design-and-secure	cloudwatch-alarm-action-che ck	Amazon CloudWatch memperingatkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasark an pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insuffici entDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-11-beban kerja material b-design-and-secure	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
bagian4 -cloud-11-beban kerja material b-design-and-secure	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
bagian4 -cloud-11-beban kerja material b-design-and-secure	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-11-beban kerja material b-design-and-secure	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
bagian4 -cloud-11-beban kerja material b-design-and-secure	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentif ikasi, Anda harus menonakti fkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-11-beban kerja material b-design-and-secure	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
bagian4 -cloud-11-beban kerja material b-design-and-secure	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-11-beban kerja material b-design-and-secure	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-11-beban kerja material b-design-and-secure	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
bagian4 -cloud-11-beban kerja material b-design-and-secure	vpc-flow-logs-enabled	Log aliran VPC menyediak an catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-11-beban kerja material b-design-and-secure	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
bagian4 -the-cloud-12-beban kerja standar b-design-and-secure	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
bagian4 -the-cloud-12-beban kerja standar b-design-and-secure	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-12-beban kerja standar b-design-and-secure	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
bagian4 -the-cloud-12-beban kerja standar b-design-and-secure	codebuild-project-envvar-awscred-periksa	Pastikan kredensyal otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild. Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.
bagian4 -the-cloud-12-beban kerja standar b-design-and-secure	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredensyal masuk dalam lingkungan proyek Codebuild. AWS Gunakan OAuth alih-alih token akses pribadi atau kredensi masuk untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-12-beban kerja standar b-design-and-secure	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
bagian4 -the-cloud-12-beban kerja standar b-design-and-secure	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
bagian4 -the-cloud-12-beban kerja standar b-design-and-secure	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-12-beban kerja standar b-design-and-secure	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
bagian4 -the-cloud-12-beban kerja standar b-design-and-secure	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
bagian4 -the-cloud-12-beban kerja standar b-design-and-secure	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-12-beban kerja standar b-design-and-secure	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
bagian4 -the-cloud-12-beban kerja standar b-design-and-secure	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-12-beban kerja standar b-design-and-secure	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.
bagian4 -the-cloud-12-beban kerja standar b-design-and-secure	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
bagian4 -the-cloud-12-beban kerja standar b-design-and-secure	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-12-beban kerja standar b-design-and-secure	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
bagian4 -the-cloud-12-beban kerja standar b-design-and-secure	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-12-beban kerja standar b-design-and-secure	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
bagian4 -the-cloud-12-beban kerja standar b-design-and-secure	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
bagian4 -the-cloud-12-beban kerja standar b-design-and-secure	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-12-beban kerja standar b-design-and-secure	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
bagian4 -cloud-14-beban kerja material b-design-and-secure	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
bagian4 -cloud-14-beban kerja material b-design-and-secure	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-14-beban kerja material b-design-and-secure	cloudwatch-alarm-action-check	Amazon CloudWatch memperingatkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.
bagian4 -cloud-14-beban kerja material b-design-and-secure	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-14-beban kerja material b-design-and-secure	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.
bagian4 -cloud-14-beban kerja material b-design-and-secure	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-14-beban kerja material b-design-and-secure	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
bagian4 -cloud-14-beban kerja material b-design-and-secure	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-14-beban kerja material b-design-and-secure	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relational Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
bagian4 -cloud-14-beban kerja material b-design-and-secure	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-14-beban kerja material b-design-and-secure	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
bagian4 -the-cloud-14-beba n kerja standar b-design-and-secure	api-gw-execution-logging-di aktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
bagian4 -the-cloud-14-beba n kerja standar b-design-and-secure	cloudtrail-s3-dataevents-di aktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
bagian4 -cloud-15-beban kerja material b-design-and-secure	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-15-beban kerja material b-design-and-secure	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
bagian4 -cloud-15-beban kerja material b-design-and-secure	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relational Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-15-beban kerja material b-design-and-secure	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
bagian4 -1-beban kerja standar c-run-the-cloud	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -2-material-beban kerja c-run-the-cloud	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.
bagian4 -2-material-beban kerja c-run-the-cloud	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapka n status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigura si aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -2-beban kerja standar c-run-the-cloud	cloudwatch-alarm-action-check	Amazon CloudWatch memperingatkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.
bagian4 -2-beban kerja standar c-run-the-cloud	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -2-beban kerja standar c-run-the-cloud	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.
bagian4 -2-beban kerja standar c-run-the-cloud	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -2-beban kerja standar c-run-the-cloud	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
bagian4 -2-beban kerja standar c-run-the-cloud	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -2-beban kerja standar c-run-the-cloud	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.
bagian4 -2-beban kerja standar c-run-the-cloud	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -2-beban kerja standar c-run-the-cloud	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurang i peluang bagi identitas untuk menerima atau mempertah ankan hak istimewa yang berlebihan.
bagian4 -2-beban kerja standar c-run-the-cloud	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -3-beban kerja standar c-run-the-cloud	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
bagian4 -3-beban kerja standar c-run-the-cloud	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
bagian4 -3-beban kerja standar c-run-the-cloud	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktif an beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -3-beban kerja standar c-run-the-cloud	cloudwatch-alarm-action-check	Amazon CloudWatch memperingatkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.
bagian4 -3-beban kerja standar c-run-the-cloud	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -3-beban kerja standar c-run-the-cloud	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penol akan dengan merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilka n, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
bagian4 -3-beban kerja standar c-run-the-cloud	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -3-beban kerja standar c-run-the-cloud	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.
bagian4 -3-beban kerja standar c-run-the-cloud	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -3-beban kerja standar c-run-the-cloud	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifka n. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.
bagian4 -3-beban kerja standar c-run-the-cloud	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -3-beban kerja standar c-run-the-cloud	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimk an file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -3-beban kerja standar c-run-the-cloud	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
bagian4 -3-beban kerja standar c-run-the-cloud	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -3-beban kerja standar c-run-the-cloud	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -3-beban kerja standar c-run-the-cloud	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
bagian4 -3-beban kerja standar c-run-the-cloud	vpc-flow-logs-enabled	Log aliran VPC menyediak an catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -3-beban kerja standar c-run-the-cloud	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
bagian4 -4-beban kerja standar c-run-the-cloud	response-plan-exists-maintained (pemeriksaan proses)	Memastikan rencana respons insiden dibuat, dipelihara, dan didistribusikan kepada personel yang bertanggung jawab.
bagian4 -4-material-beban kerja c-run-the-cloud	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -4-material-beban kerja c-run-the-cloud	api-gw-associated-with-waf	AWS WAF memungkin kan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindung inya dari serangan berbahaya
bagian4 -4-material-beban kerja c-run-the-cloud	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -4-material-beban kerja c-run-the-cloud	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -5-beban kerja standar c-run-the-cloud	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.
bagian4 -5-beban kerja standar c-run-the-cloud	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -5-beban kerja standar c-run-the-cloud	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -5-beban kerja standar c-run-the-cloud	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -5-beban kerja standar c-run-the-cloud	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.
bagian4 -5-beban kerja standar c-run-the-cloud	lambda-concurrency-check	Aturan ini memastikan bahwa batas tinggi dan rendah konkurensi fungsi Lambda ditetapkan. Ini dapat membantu dalam menyusun dasar jumlah permintaan yang dilayani oleh fungsi Anda pada waktu tertentu.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -5-beban kerja standar c-run-the-cloud	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -5-beban kerja standar c-run-the-cloud	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -6-beban kerja material c-run-the-cloud	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.
bagian4 -6-beban kerja material c-run-the-cloud	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapka n status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigura si aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -6-beban kerja material c-run-the-cloud	ec2- -periksa managedin stance-patch-compliance-sta tus	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
bagian4 -6-beban kerja material c-run-the-cloud	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -6-beban kerja material c-run-the-cloud	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan: rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -6-beban kerja standar c-run-the-cloud	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.
bagian4 -6-beban kerja standar c-run-the-cloud	ec2- -periksa managedin stance-patch-compliance-sta tus	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -6-beban kerja standar c-run-the-cloud	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00 -sat: 16:30), dan automated SnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -6-beban kerja standar c-run-the-cloud	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Beban Kerja Material ABS CCIG 2.0.

Praktik Terbaik Operasional untuk Beban Kerja Standar ABS CCIG 2.0

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini menyediakan contoh pemetaan antara ABS Cloud Computing Implementation Guide 2.0 - Beban Kerja Standar dan aturan AWS Config terkelola. Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau beberapa kontrol Panduan Implementasi Komputasi Awan ABS. Kontrol Panduan Implementasi Komputasi Awan ABS dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -2-beban kerja standar a-govern-the-cloud	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organ izations membantu memastika n bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabk an konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.
bagian4 -2-beban kerja standar a-govern-the-cloud	cloudtrail-s3-dataevents-di aktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali

ID Kontrol	AWS Aturan Config	Bimbingan
		apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
bagian4 -2-beban kerja standar a-govern-the-cloud	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktif an beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -2-beban kerja standar a-govern-the-cloud	cloudwatch-alarm-action-check	Amazon CloudWatch memperingatkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.
bagian4 -2-beban kerja standar a-govern-the-cloud	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -2-beban kerja standar a-govern-the-cloud	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.
bagian4 -2-beban kerja standar a-govern-the-cloud	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -2-beban kerja standar a-govern-the-cloud	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
bagian4 -3-beban kerja standar a-govern-the-cloud	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -3-beban kerja standar a-govern-the-cloud	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan , sesuai dengan standar organisasi Anda.
bagian4 -3-beban kerja standar a-govern-the-cloud	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirk an ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -3-beban kerja standar a-govern-the-cloud	terlampir eip	Aturan ini memastikan Elastic IPs dialokasikan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan . Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.
bagian4 -3-beban kerja standar a-govern-the-cloud	vpc-network-acl-unused-periksa	Aturan ini memastikan bahwa daftar kontrol akses jaringan Amazon Virtual Private Cloud (VPC) sedang digunakan . Pemantauan untuk daftar kontrol akses jaringan yang tidak digunakan dapat membantu inventaris dan pengelolaan lingkungan Anda yang akurat.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribus i kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertah ankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi, pengembalian, dan pendelegasian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigurasi ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositori data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	ecs-containers-nonprivileged	Untuk membantu menerapkan prinsip hak istimewa paling rendah, definisi tugas Amazon Elastic Container Service (Amazon ECS) seharusnya tidak mengaktifkan hak istimewa yang ditinggikan. Ketika parameter ini benar, wadah diberikan hak istimewa yang ditinggikan pada instance wadah host (mirip dengan pengguna root).
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	ecs-containers-readonly-access	Mengaktifkan akses baca saja ke kontainer Amazon Elastic Container Service (ECS) dapat membantu mematuhi prinsip hak istimewa yang paling rendah. Opsi ini dapat mengurangi vektor serangan karena sistem file instance container tidak dapat dimodifikasi kecuali jika memiliki izin baca-tulis eksplisit.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	opensearch-access-control-enabled	Pastikan kontrol akses berbutir halus diaktifkan di domain Layanan Amazon OpenSearch Anda. Kontrol akses berbutir halus menyediakan mekanisme otorisasi yang disempurnakan untuk mencapai akses yang paling tidak memiliki hak istimewa ke domain Layanan Amazon. OpenSearch Ini memungkinkan kontrol akses berbasis peran ke domain, serta indeks, dokumen, dan keamanan tingkat lapangan, dukungan untuk dasbor OpenSearch Layanan multi-tenancy, dan otentikasi dasar HTTP untuk Layanan dan Kibana. OpenSearch
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-1-standard-beban kerja b-design-and-secure	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
bagian4 -the-cloud-2-beban kerja standar b-design-and-secure	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-2-beban kerja standar b-design-and-secure	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.
bagian4 -the-cloud-2-beban kerja standar b-design-and-secure	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapka n status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigura si aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-2-beban kerja standar b-design-and-secure	ec2- -periksa managedin stance-patch-compliance-sta tus	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
bagian4 -the-cloud-2-beban kerja standar b-design-and-secure	redshift-cluster-maintenanc esettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengatura n yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrad e. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00 -sat: 16:30), dan automated SnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-3-standard-beban kerja b-design-and-secure	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.
bagian4 -the-cloud-3-standard-beban kerja b-design-and-secure	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-3-standard-beban kerja b-design-and-secure	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.
bagian4 -the-cloud-3-standard-beban kerja b-design-and-secure	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-3-standard-beban kerja b-design-and-secure	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
bagian4 -the-cloud-3-standard-beban kerja b-design-and-secure	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-3-standard-beban kerja b-design-and-secure	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-3-standard-beban kerja b-design-and-secure	rds-cluster-multi-az-diaktifkan	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-3-standard-beban kerja b-design-and-secure	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	api-gw-associated-with-waf	AWS WAF memungkin kan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindung inya dari serangan berbahaya
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearc h Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribus i kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertah ankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabun gkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandun g tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkin kan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizink an tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi, pengembalian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedAc tionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurang i peluang bagi identitas untuk menerima atau mempertah ankan hak istimewa yang berlebihan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentif ikasi, Anda harus menonakti fkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkin kan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabk an akses tidak sah ke sumber daya VPC Amazon.
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	lambda-function-public-acce ss-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyarat an untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearc h Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,338 9,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	sagemaker-notebook-no-direc t-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimpleme ntasikan untuk mencapai persyaratan ketahanan . Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-S ite VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	s3- -dilarang bucket-level-publi c-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-4-beban kerja standar b-design-and-secure	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
bagian4 -the-cloud-5-standard-beban kerja b-design-and-secure	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -the-cloud-5-standard-beban kerja b-design-and-secure	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-5-standard-beban kerja b-design-and-secure	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-5-standard-beban kerja b-design-and-secure	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi, pengembalian, dan pendelegasian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-5-standard-beban kerja b-design-and-secure	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
bagian4 -the-cloud-5-standard-beban kerja b-design-and-secure	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	alb-http-drop-invalid-Header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-6-beban kerja standar b-design-and-secure	alb-http-to-https-pengalihan-periksa	Untuk membantu melindung i data dalam perjalanan, pastikan bahwa Applicati on Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	api-gw-cache-enabled-dan-di enkripsi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	cloudwatch-log-group-encryp ted	Untuk membantu melindung i data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-6-beban kerja standar b-design-and-secure	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-6-beban kerja standar b-design-and-secure	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-6-beban kerja standar b-design-and-secure	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan membantu melindung i data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindung i data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-6-beban kerja standar b-design-and-secure	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	kinesis-stream-encrypted	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	kinesis-stream-encrypted	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-6-beban kerja standar b-design-and-secure	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-6-beban kerja standar b-design-and-secure	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-6-beban kerja standar b-design-and-secure	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	s3- bucket-ssl-requests-only	Untuk membantu melindung i data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerluka n permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-6-beban kerja standar b-design-and-secure	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-6-beban kerja standar b-design-and-secure	sns-encrypted-kms	Untuk membantu melindung i data saat istirahat, pastikan topik Amazon Simple Notificat ion Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifika t SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
bagian4 -cloud-6-beban kerja standar b-design-and-secure	redshift-cluster-kms-enabled	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-8-beban kerja standar b-design-and-secure	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaima na ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -cloud-8-beban kerja standar b-design-and-secure	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organ izations membantu memastika n bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabk an konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-8-beban kerja standar b-design-and-secure	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktif an beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-8-beban kerja standar b-design-and-secure	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribus i kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertah ankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-8-beban kerja standar b-design-and-secure	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-8-beban kerja standar b-design-and-secure	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-8-beban kerja standar b-design-and-secure	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizink an tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi, pengembalian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedAc tionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-8-beban kerja standar b-design-and-secure	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-8-beban kerja standar b-design-and-secure	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -cloud-8-beban kerja standar b-design-and-secure	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
bagian4 -cloud-8-beban kerja standar b-design-and-secure	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-8-beban kerja standar b-design-and-secure	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.
bagian4 -cloud-8-beban kerja standar b-design-and-secure	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-8-beban kerja standar b-design-and-secure	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
bagian4 -cloud-8-beban kerja standar b-design-and-secure	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurang i peluang bagi identitas untuk menerima atau mempertah ankan hak istimewa yang berlebihan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-8-beban kerja standar b-design-and-secure	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentif ikasi, Anda harus menonakti fkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-8-beban kerja standar b-design-and-secure	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
bagian4 -cloud-8-beban kerja standar b-design-and-secure	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -cloud-8-beban kerja standar b-design-and-secure	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifka n untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
bagian4 -the-cloud-9-beban kerja standar b-design-and-secure	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penol akan dengan merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilka n, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-9-beban kerja standar b-design-and-secure	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.
bagian4 -the-cloud-9-beban kerja standar b-design-and-secure	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-9-beban kerja standar b-design-and-secure	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
bagian4 -the-cloud-9-beban kerja standar b-design-and-secure	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-9-beban kerja standar b-design-and-secure	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.
bagian4 -the-cloud-9-beban kerja standar b-design-and-secure	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-9-beban kerja standar b-design-and-secure	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
bagian4 -the-cloud-9-beban kerja standar b-design-and-secure	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurang i peluang bagi identitas untuk menerima atau mempertah ankan hak istimewa yang berlebihan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-9-beban kerja standar b-design-and-secure	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentif ikasi, Anda harus menonakti fkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-9-beban kerja standar b-design-and-secure	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
bagian4 -the-cloud-9-beban kerja standar b-design-and-secure	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-9-beban kerja standar b-design-and-secure	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifka n untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
bagian4 -the-cloud-9-beban kerja standar b-design-and-secure	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigurasi ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-10-beban kerja standar b-design-and-secure	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
bagian4 -the-cloud-12-standard-beban kerja b-design-and-secure	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
bagian4 -the-cloud-12-standard-beban kerja b-design-and-secure	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
bagian4 -the-cloud-12-standard-beban kerja b-design-and-secure	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-12-standard-beban kerja b-design-and-secure	codebuild-project-envvar-awscred-periksa	Pastikan kredensyal otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild. Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.
bagian4 -the-cloud-12-standard-beban kerja b-design-and-secure	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredenal masuk dalam lingkungan proyek Codebuild. AWS Gunakan OAuth alih-alih token akses pribadi atau kredensyal masuk untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-12-standard-beban kerja b-design-and-secure	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
bagian4 -the-cloud-12-standard-beban kerja b-design-and-secure	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
bagian4 -the-cloud-12-standard-beban kerja b-design-and-secure	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-12-standard-beban kerja b-design-and-secure	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
bagian4 -the-cloud-12-standard-beban kerja b-design-and-secure	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
bagian4 -the-cloud-12-standard-beban kerja b-design-and-secure	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-12-standard-beban kerja b-design-and-secure	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
bagian4 -the-cloud-12-standard-beban kerja b-design-and-secure	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-12-standard-beban kerja b-design-and-secure	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.
bagian4 -the-cloud-12-standard-beban kerja b-design-and-secure	kinesis-stream-encrypted	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.
bagian4 -the-cloud-12-standard-beban kerja b-design-and-secure	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-12-standard-beban kerja b-design-and-secure	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
bagian4 -the-cloud-12-standard-beban kerja b-design-and-secure	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-12-standard-beban kerja b-design-and-secure	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -the-cloud-12-standard-beban kerja b-design-and-secure	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-12-standard-beban kerja b-design-and-secure	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
bagian4 -the-cloud-12-standard-beban kerja b-design-and-secure	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-12-standard-beban kerja b-design-and-secure	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-14-beba n kerja standar b-design-and-secure	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.
bagian4 -the-cloud-14-beba n kerja standar b-design-and-secure	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_ bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
bagian4 -the-cloud-14-beban kerja standar b-design-and-secure	opensearch-audit-logging-enabled	Pastikan pencatatan audit diaktifkan di domain OpenSearch Layanan Amazon Anda. Pencatatan audit memungkinkan Anda melacak aktivitas pengguna di OpenSearch domain Anda, termasuk keberhasilan dan kegagalan otentikasi, permintaan, perubahan indeks OpenSearch, dan kueri penelusuran yang masuk.
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -the-cloud-15-beban kerja standar b-design-and-secure	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
bagian4 -1-beban kerja standar c-run-the-cloud	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -2-beban kerja standar c-run-the-cloud	cloudwatch-alarm-action-check	Amazon CloudWatch memperingatkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.
bagian4 -2-beban kerja standar c-run-the-cloud	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -2-beban kerja standar c-run-the-cloud	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.
bagian4 -2-beban kerja standar c-run-the-cloud	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -2-beban kerja standar c-run-the-cloud	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
bagian4 -2-beban kerja standar c-run-the-cloud	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -2-beban kerja standar c-run-the-cloud	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.
bagian4 -2-beban kerja standar c-run-the-cloud	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -2-beban kerja standar c-run-the-cloud	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurang i peluang bagi identitas untuk menerima atau mempertah ankan hak istimewa yang berlebihan.
bagian4 -2-beban kerja standar c-run-the-cloud	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -3-beban kerja standar c-run-the-cloud	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
bagian4 -3-beban kerja standar c-run-the-cloud	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
bagian4 -3-beban kerja standar c-run-the-cloud	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktif an beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -3-beban kerja standar c-run-the-cloud	cloudwatch-alarm-action-check	Amazon CloudWatch memperingatkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.
bagian4 -3-beban kerja standar c-run-the-cloud	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -3-beban kerja standar c-run-the-cloud	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penol akan dengan merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilka n, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
bagian4 -3-beban kerja standar c-run-the-cloud	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -3-beban kerja standar c-run-the-cloud	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.
bagian4 -3-beban kerja standar c-run-the-cloud	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -3-beban kerja standar c-run-the-cloud	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifka n. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.
bagian4 -3-beban kerja standar c-run-the-cloud	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -3-beban kerja standar c-run-the-cloud	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimk an file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -3-beban kerja standar c-run-the-cloud	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
bagian4 -3-beban kerja standar c-run-the-cloud	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -3-beban kerja standar c-run-the-cloud	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -3-beban kerja standar c-run-the-cloud	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -3-beban kerja standar c-run-the-cloud	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
bagian4 -3-beban kerja standar c-run-the-cloud	vpc-flow-logs-enabled	Log aliran VPC menyediak an catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -3-beban kerja standar c-run-the-cloud	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
bagian4 -3-beban kerja standar c-run-the-cloud	opensearch-audit-logging-enabled	Pastikan pencatatan audit diaktifkan di domain OpenSearch Layanan Amazon Anda. Pencatatan audit memungkinkan Anda melacak aktivitas pengguna di OpenSearch domain Anda, termasuk keberhasilan dan kegagalan otentikasi, permintaan, perubahan indeks OpenSearch, dan kueri penelusuran yang masuk.
bagian4 -4-beban kerja standar c-run-the-cloud	response-plan-exists-maintained (pemeriksaan proses)	Memastikan rencana respons insiden dibuat, dipelihara, dan didistribusikan kepada personel yang bertanggung jawab.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -5-beban kerja standar c-run-the-cloud	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.
bagian4 -5-beban kerja standar c-run-the-cloud	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -5-beban kerja standar c-run-the-cloud	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -5-beban kerja standar c-run-the-cloud	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -5-beban kerja standar c-run-the-cloud	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.
bagian4 -5-beban kerja standar c-run-the-cloud	lambda-concurrency-check	Aturan ini memastikan bahwa batas tinggi dan rendah konkurensi fungsi Lambda ditetapkan. Ini dapat membantu dalam menyusun dasar jumlah permintaan yang dilayani oleh fungsi Anda pada waktu tertentu.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -5-beban kerja standar c-run-the-cloud	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -5-beban kerja standar c-run-the-cloud	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -6-beban kerja standar c-run-the-cloud	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.
bagian4 -6-beban kerja standar c-run-the-cloud	ec2- -periksa managedin stance-patch-compliance-sta tus	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
bagian4 -6-beban kerja standar c-run-the-cloud	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00 -sat: 16:30), dan automated SnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
bagian4 -6-beban kerja standar c-run-the-cloud	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Beban Kerja Standar ABS CCIG 2.0.

Praktik Terbaik Operasional untuk ACSC Essential 8

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara Australian Cyber Security Centre (ACSC) Essential Eight Maturity Model dan aturan AWS Config terkelola. Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan berhubungan dengan satu atau beberapa kontrol Esential Eight ACSC. Kontrol Esential Eight ACSC dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini. Beberapa pemetaan ke aturan konfigurasi adalah untuk bagian urutan yang lebih tinggi (mis. Strategi Mitigasi untuk Membatasi Luas Insiden Keamanan Cyber) sebagai lawan dari bagian yang lebih preskriptif.

Templat paket kesesuaian sampel ini berisi pemetaan ke kontrol dalam ACSC Essential 8, yang dibuat oleh Persemakmuran Australia dan dapat ditemukan di ACSC | Essential Eight. Lisensi kerangka kerja di bawah Lisensi Publik Internasional Creative Commons Attribution 4.0 dan informasi hak cipta untuk kerangka kerja (termasuk penafian jaminan) dapat ditemukan di ACSC | Hak Cipta.

ID Kontrol	AWS Aturan Config	Bimbingan
Aplikasi_kontrol	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan,

ID Kontrol	AWS Aturan Config	Bimbingan
		membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.
Aplikasi_kontrol	api-gw-associated-with-waf	AWS WAF memungkin kan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindung inya dari serangan berbahaya

ID Kontrol	AWS Aturan Config	Bimbingan
Aplikasi_kontrol	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.
Aplikasi_kontrol	waf-regional-rule-not-kosong	Pastikan AWS WAF Anda memiliki aturan yang tidak kosong. Aturan tanpa kondisi dapat mengakibatkan perilaku yang tidak diinginkan.
Aplikasi_kontrol	waf-regional-rulegroup-not-kosong	Pastikan AWS WAF Anda memiliki grup aturan yang tidak kosong. Grup aturan yang kosong dapat mengakiba tkan perilaku yang tidak diinginkan.

ID Kontrol	AWS Aturan Config	Bimbingan
Aplikasi_kontrol	waf-regional-webacl-not-kosong	Web ACL yang dilampirkan ke AWS WAF dapat berisi kumpulan aturan dan kelompok aturan untuk memeriksa dan mengontrol permintaan web. Jika ACL Web kosong, lalu lintas web lewat tanpa terdeteksi atau ditindaklanjuti oleh WAF.
Aplikasi_kontrol	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Patch_aplikasi	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunak an kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.
Patch_aplikasi	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Patch_aplikasi	ecs-fargate-latest-platform-versi	Pembaruan dan tambalan keamanan diterapkan secara otomatis untuk tugas Fargate AWS Anda. Jika ditemukan masalah keamanan yang memengaruhi versi platform AWS Fargate, AWS tambal versi platform. Untuk membantu pengelolaan tambalan tugas Amazon Elastic Container Service (ECS) yang menjalankan AWS Fargate, perbarui tugas mandiri layanan Anda untuk menggunakan versi platform terbaru.
Patch_aplikasi	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	AWS Aturan Config	Bimbingan
Patch_aplikasi	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relationa l Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.
Patch_aplikasi	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapka n status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigura si aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Patch_aplikasi	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
RESTRICT_ADMINISTRATIVE_PRIVILEGES	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	AWS Aturan Config	Bimbingan
RESTRICT_ADMINISTRATIVE_PRIVILEGES	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
RESTRICT_ADMINISTRATIVE_PRIVILEGES	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	AWS Aturan Config	Bimbingan
RESTRICT_ADMINISTRATIVE_PRIVILEGES	codebuild-project-environment-privileged-periksa	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan lingkungan CodeBuild proyek Amazon Anda tidak mengaktifkan mode istimewa. Pengaturan ini harus dinonaktifkan untuk mencegah akses yang tidak diinginkan ke Docker APIs serta perangkat keras yang mendasarinya.
RESTRICT_ADMINISTRATIVE_PRIVILEGES	ecs-containers-nonprivileged	Untuk membantu menerapkan prinsip hak istimewa paling rendah, definisi tugas Amazon Elastic Container Service (Amazon ECS) seharusnya tidak mengaktifkan hak istimewa yang ditinggikan. Ketika parameter ini benar, wadah diberikan hak istimewa yang ditinggikan pada instance wadah host (mirip dengan pengguna root).

ID Kontrol	AWS Aturan Config	Bimbingan
RESTRICT_ADMINISTRATIVE_PRIVILEGES	ecs-containers-readonly-access	Mengaktifkan akses baca saja ke kontainer Amazon Elastic Container Service (ECS) dapat membantu mematuhi prinsip hak istimewa yang paling rendah. Opsi ini dapat mengurangi vektor serangan karena sistem file instance container tidak dapat dimodifikasi kecuali jika memiliki izin baca-tulis eksplisit.
RESTRICT_ADMINISTRATIVE_PRIVILEGES	ecs-task-definition-nonroot-pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan bahwa pengguna non-root ditunjuk untuk mengakses definisi tugas Amazon Elastic Container Service (Amazon ECS) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
RESTRICT_ADMINISTRATIVE_PRIVILEGES	efs-access-point-enforce-identitas pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan penegakan pengguna diaktifkan untuk Amazon Elastic File System (Amazon EFS) Anda. Saat diaktifkan, Amazon EFS menggantikan pengguna dan grup klien NFS IDs dengan identitas yang dikonfigurasi pada titik akses untuk semua operasi sistem file dan hanya memberikan akses ke identitas pengguna yang diberlakukan ini.
RESTRICT_ADMINISTRATIVE_PRIVILEGES	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
RESTRICT_ADMINISTRATIVE_PRIVILEGES	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
RESTRICT_ADMINISTRATIVE_PRIVILEGES	rds-instance-iam-authentication-diaktifkan	Pastikan autentikasi AWS Identity and Access Management (IAM) diaktifkan pada instans Amazon Relational Database Service (Amazon RDS) untuk mengontrol akses ke sistem dan aset. Ini memberlakukan lalu lintas jaringan ke dan dari database yang akan dienkripsi menggunakan Secure Sockets Layer (SSL). Anda tidak diharuskan untuk menyimpan kredensi pengguna dalam database, karena otentikasi dikelola secara eksternal.
RESTRICT_ADMINISTRATIVE_PRIVILEGES	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
RESTRICT_ADMINISTRATIVE_PRIVILEGES	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	AWS Aturan Config	Bimbingan
RESTRICT_ADMINISTRATIVE_PRIVILEGES	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda

ID Kontrol	AWS Aturan Config	Bimbingan
RESTRICT_ADMINISTRATIVE_PRIVILEGES	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi, pengembalian, dan pendelegasian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
RESTRICT_ADMINISTRATIVE_PRIVILEGES	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
Patch_Operating_Systems	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Multi-faktor_otentikasi	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.
Multi-faktor_otentikasi	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
Multi-faktor_otentikasi	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
Multi-faktor_otentikasi	root-account-hardware-mfa-d iaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
Multi-faktor_otentikasi	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifka n untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
Regular_backup	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Regular_backup	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
Regular_backup	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Regular_backup	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
Regular_backup	elasticache-redis-cluster-a utomatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCac he membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentuka n oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	AWS Aturan Config	Bimbingan
Regular_backup	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relational Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
Regular_backup	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersedi aan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	AWS Aturan Config	Bimbingan
Regular_backup	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihka n setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.
Regular_backup	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Regular_backup	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Regular_backup	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.
Regular_backup	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Regular_backup	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk ACSC Essential 8.

Praktik Terbaik Operasional untuk ACSC ISM

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara Australian Cyber Security Centre (ACSC) Information Security Manual (ISM) 2020-06 dan aturan AWS Config terkelola. Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan berhubungan dengan satu atau beberapa kontrol ISM. Kontrol ISM dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

Templat paket kesesuaian sampel ini berisi pemetaan ke kontrol dalam kerangka kerja ISM, yang dibuat oleh Persemakmuran Australia dan dapat ditemukan di Manual Keamanan Informasi Pemerintah Australia. Lisensi kerangka kerja di bawah Lisensi Publik Internasional Creative Commons Attribution 4.0 dan informasi hak cipta untuk kerangka kerja (termasuk penafian jaminan) dapat ditemukan di ACSC | Hak Cipta.

ID Kontrol	AWS Aturan Config	Bimbingan
43	response-plan-exists-maintained (pemeriksaan proses)	Memastikan rencana respons insiden dibuat, dipelihara, dan didistribusikan kepada personel yang bertanggung jawab.
252	security-awareness-program-exists (pemeriksaan proses)	Membangun dan memelihara program kesadaran keamanan untuk organisasi Anda. Program kesadaran keamanan mendidik karyawan tentang cara melindungi organisasi mereka dari berbagai pelanggaran atau insiden keamanan.
261	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
261	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan

ID Kontrol	AWS Aturan Config	Bimbingan
		memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.
261	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
298	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
298	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00 -sat: 16:30), dan automated SnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
298	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	AWS Aturan Config	Bimbingan
298	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relationa l Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.
380	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabun gkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
459	api-gw-cache-enabled-dan-di enkripsi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
459	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
459	ec2- ebs-encryption-by-default	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
459	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
459	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
459	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
459	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
459	redshift-cluster-kms-enabled	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
459	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
459	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
459	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
459	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
459	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
459	codebuild-project-artifact-encryption	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk AWS CodeBuild artefak Anda.
459	codebuild-project-s3-log-terenkripsi	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk AWS CodeBuild log Anda yang disimpan di Amazon S3.
459	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
459	kinesis-stream-encrypted	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
459	rds-snapshot-encrypted	Pastikan enkripsi diaktifka n untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
459	rds-storage-encrypted	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
459	sns-encrypted-kms	Untuk membantu melindung i data saat istirahat, pastikan topik Amazon Simple Notificat ion Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
580	audit-log-policy-exists (pemeriksaan proses)	Menetapkan dan memelihar a kebijakan manajemen log audit yang menentuka n persyaratan pencatatan organisasi Anda. Ini termasuk, namun tidak terbatas pada, peninjauan dan retensi log audit.
634	vpc-flow-logs-enabled	Log aliran VPC menyediak an catatan terperinci untuk informasi tentang lalu lintas IP yang pergi ke dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
859	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	AWS Aturan Config	Bimbingan
974	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
974	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahk an lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
1139	elb-predefined-security-policy-ssl-periksa	Untuk membantu melindung i data dalam perjalanan, pastikan bahwa pendengar SSL Classic Elastic Load Balancing Anda menggunak an kebijakan keamanan yang telah ditentukan sebelumny a. Elastic Load Balancing menyediakan konfigurasi negosiasi SSL yang telah ditentukan sebelumny a yang digunakan untuk negosiasi SSL ketika koneksi dibuat antara klien dan penyeimbang beban Anda. Konfigurasi negosiasi SSL memberikan kompatibilitas dengan berbagai klien dan menggunakan algoritma kriptografi berkekuatan tinggi. Aturan ini mengharus kan Anda menetapkan kebijakan keamanan yang telah ditentukan untuk pendengar SSL Anda. Kebijakan keamanan default adalah: ELBSecurity Policy-TLS-1-2-2017-0. Nilai aktual harus mencerminkan kebijakan organisasi Anda

ID Kontrol	AWS Aturan Config	Bimbingan
1173	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
1173	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
1173	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.
1173	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
1173	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahk an lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
1228	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1240	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.
1240	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindungiinya dari serangan berbahaya

ID Kontrol	AWS Aturan Config	Bimbingan
1271	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
1271	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositori data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	AWS Aturan Config	Bimbingan
1277	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
1277	rds-instance-iam-authentication-diaktifkan	Pastikan autentikasi AWS Identity and Access Management (IAM) diaktifkan pada instans Amazon Relational Database Service (Amazon RDS) untuk mengontrol akses ke sistem dan aset. Ini memberlakukan lalu lintas jaringan ke dan dari database yang akan dienkripsi menggunakan Secure Sockets Layer (SSL). Anda tidak diharuskan untuk menyimpan kredensi pengguna dalam database, karena otentikasi dikelola secara eksternal.
1277	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.

ID Kontrol	AWS Aturan Config	Bimbingan
1380	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunak an kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.
1380	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1380	ecs-fargate-latest-platform-versi	Pembaruan dan tambalan keamanan diterapkan secara otomatis untuk tugas Fargate AWS Anda. Jika ditemukan masalah keamanan yang memengaruhi versi platform AWS Fargate, AWS tambal versi platform. Untuk membantu pengelolaan tambalan tugas Amazon Elastic Container Service (ECS) yang menjalankan AWS Fargate, perbarui tugas mandiri layanan Anda untuk menggunakan versi platform terbaru.
1380	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	AWS Aturan Config	Bimbingan
1380	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relationa l Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.
1380	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapka n status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigura si aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1380	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1380	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	AWS Aturan Config	Bimbingan
1380	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
1380	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	AWS Aturan Config	Bimbingan
1380	codebuild-project-environment-privileged-periksa	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan lingkungan CodeBuild proyek Amazon Anda tidak mengaktifkan mode istimewa. Pengaturan ini harus dinonaktifkan untuk mencegah akses yang tidak diinginkan ke Docker APIs serta perangkat keras yang mendasarinya.
1380	ecs-containers-nonprivileged	Untuk membantu menerapkan prinsip hak istimewa paling rendah, definisi tugas Amazon Elastic Container Service (Amazon ECS) seharusnya tidak mengaktifkan hak istimewa yang ditinggikan. Ketika parameter ini benar, wadah diberikan hak istimewa yang ditinggikan pada instance wadah host (mirip dengan pengguna root).

ID Kontrol	AWS Aturan Config	Bimbingan
1380	ecs-containers-readonly-access	Mengaktifkan akses baca saja ke wadah Amazon Elastic Container Service (ECS) dapat membantu mematuhi prinsip hak istimewa yang paling rendah. Opsi ini dapat mengurangi vektor serangan karena sistem file instance container tidak dapat dimodifikasi kecuali jika memiliki izin baca-tulis eksplisit.
1380	ecs-task-definition-nonroot-pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan bahwa pengguna non-root ditunjuk untuk mengakses definisi tugas Amazon Elastic Container Service (Amazon ECS) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1380	efs-access-point-enforce-id entitas pengguna	Untuk membantu menerapka n prinsip hak istimewa paling sedikit, pastikan penegakan pengguna diaktifkan untuk Amazon Elastic File System (Amazon EFS) Anda. Saat diaktifkan, Amazon EFS menggantikan pengguna dan grup klien NFS IDs dengan identitas yang dikonfigu rasi pada titik akses untuk semua operasi sistem file dan hanya memberikan akses ke identitas pengguna yang diberlakukan ini.
1380	iam-user-group-membership-p eriksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
1380	rds-instance-iam-authentication-diaktifkan	Pastikan autentikasi AWS Identity and Access Management (IAM) diaktifkan pada instans Amazon Relational Database Service (Amazon RDS) untuk mengontrol akses ke sistem dan aset. Ini memberlakukan lalu lintas jaringan ke dan dari database yang akan dienkripsi menggunakan Secure Sockets Layer (SSL). Anda tidak diharuskan untuk menyimpan kredensi pengguna dalam database, karena otentikasi dikelola secara eksternal.
1380	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
1380	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	AWS Aturan Config	Bimbingan
1380	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabun gkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandun g tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkin kan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda

ID Kontrol	AWS Aturan Config	Bimbingan
1380	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizink an tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi, pengembalian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedAc tionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1380	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkin kan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
1388	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,338 9,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1388	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.
1401	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	AWS Aturan Config	Bimbingan
1401	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
1401	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahk an lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
1401	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
1401	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
1402	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
1404	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentif ikasi, Anda harus menonakti fkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
1405	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatc h untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaa n AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	AWS Aturan Config	Bimbingan
1405	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penol akan dengan merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilka n, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
1405	multi-region-cloudtrail-enabled	MULTI_REGION_CLOUD _TRAIL_ENABLED
1405	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktif an beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	AWS Aturan Config	Bimbingan
1405	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
1405	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
1405	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	AWS Aturan Config	Bimbingan
1405	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
1405	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1405	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.
1405	vpc-flow-logs-enabled	Log aliran VPC menyediak an catatan terperinci untuk informasi tentang lalu lintas IP yang pergi ke dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	AWS Aturan Config	Bimbingan
1405	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
1405	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	AWS Aturan Config	Bimbingan
1405	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.
1405	redshift-audit-logging-enabled	Untuk menangkap informasi tentang koneksi dan aktivitas pengguna di klaster Amazon Redshift, pastikan pencatatan audit diaktifkan.
1405	opensearch-audit-logging-enabled	Pastikan pencatatan audit diaktifkan di domain OpenSearch Layanan Amazon Anda. Pencatatan audit memungkinkan Anda melacak aktivitas pengguna di OpenSearch domain Anda, termasuk keberhasilan dan kegagalan otentikasi, permintaan, perubahan indeks OpenSearch, dan kueri penelusuran yang masuk.

ID Kontrol	AWS Aturan Config	Bimbingan
1405	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
1490	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1490	api-gw-associated-with-waf	AWS WAF memungkin kan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindung inya dari serangan berbahaya
1490	waf-regional-rule-not-kosong	Pastikan AWS WAF Anda memiliki aturan yang tidak kosong. Aturan tanpa kondisi dapat mengakibatkan perilaku yang tidak diinginkan.
1490	waf-regional-rulegroup-not-kosong	Pastikan AWS WAF Anda memiliki grup aturan yang tidak kosong. Grup aturan yang kosong dapat mengakiba tkan perilaku yang tidak diinginkan.

ID Kontrol	AWS Aturan Config	Bimbingan
1490	waf-regional-webacl-not-kosong	Web ACL yang dilampirkan ke AWS WAF dapat berisi kumpulan aturan dan kelompok aturan untuk memeriksa dan mengontrol permintaan web. Jika ACL Web kosong, lalu lintas web lewat tanpa terdeteksi atau ditindaklanjuti oleh WAF.
1490	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1501	ec2- -periksa managedin stance-patch-compliance-sta tus	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
1504	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	AWS Aturan Config	Bimbingan
1504	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
1504	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahk an lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
1504	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
1504	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
1509	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
1509	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	AWS Aturan Config	Bimbingan
1509	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimk an file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
1509	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktif an beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.
1509	elasticsearch-logs-to-cloud watch	Pastikan domain OpenSearc h Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersediaan.
1509	api-gw-execution-logging-di aktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
1509	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
1509	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	AWS Aturan Config	Bimbingan
1509	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDbEncrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1509	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.
1509	vpc-flow-logs-enabled	Log aliran VPC menyediak an catatan terperinci untuk informasi tentang lalu lintas IP yang pergi ke dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	AWS Aturan Config	Bimbingan
1509	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
1509	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	AWS Aturan Config	Bimbingan
1509	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.
1509	redshift-audit-logging-enabled	Untuk menangkap informasi tentang koneksi dan aktivitas pengguna di klaster Amazon Redshift, pastikan pencatatan audit diaktifkan.
1509	opensearch-audit-logging-enabled	Pastikan pencatatan audit diaktifkan di domain OpenSearch Layanan Amazon Anda. Pencatatan audit memungkinkan Anda melacak aktivitas pengguna di OpenSearch domain Anda, termasuk keberhasilan dan kegagalan otentikasi, permintaan, perubahan indeks OpenSearch, dan kueri penelusuran yang masuk.

ID Kontrol	AWS Aturan Config	Bimbingan
1509	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
1511	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1511	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
1511	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan cadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	AWS Aturan Config	Bimbingan
1511	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
1511	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1511	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.
1511	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relational Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1511	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihka n setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.
1511	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	AWS Aturan Config	Bimbingan
1511	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1511	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1511	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1511	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
1511	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1511	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersedi aan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	AWS Aturan Config	Bimbingan
1511	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1511	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.
1515	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1515	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
1515	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1515	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
1515	elasticache-redis-cluster-a utomatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCac he membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentuka n oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	AWS Aturan Config	Bimbingan
1515	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relational Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
1515	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersedi aan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	AWS Aturan Config	Bimbingan
1515	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihka n setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.
1515	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1515	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1515	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.
1515	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1515	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.
1536	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	AWS Aturan Config	Bimbingan
1537	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
1537	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1552	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
1552	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
1552	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certifica te Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
1552	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
1552	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certifica te Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	AWS Aturan Config	Bimbingan
1579	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.
1580	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	AWS Aturan Config	Bimbingan
1580	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independe n yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
1580	rds-cluster-multi-az-diaktifkan	Cluster Amazon Relational Database Service (Amazon RDS) harus mengaktifkan replikasi Multi-AZ untuk membantu ketersediaan data yang disimpan. Setiap Availability Zone berjalan pada infrastruktur independe n yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.
1650	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatc h untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaa n AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	AWS Aturan Config	Bimbingan
1650	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penol akan dengan merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilka n, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	AWS Aturan Config	Bimbingan
1650	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimk an file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
1650	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktif an beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.
1650	elasticsearch-logs-to-cloud watch	Pastikan domain OpenSearc h Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersediaan.
1650	api-gw-execution-logging-di aktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
1650	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
1650	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	AWS Aturan Config	Bimbingan
1650	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1650	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.
1650	vpc-flow-logs-enabled	Log aliran VPC menyediak an catatan terperinci untuk informasi tentang lalu lintas IP yang pergi ke dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	AWS Aturan Config	Bimbingan
1650	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
1650	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	AWS Aturan Config	Bimbingan
1650	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.
1650	redshift-audit-logging-enabled	Untuk menangkap informasi tentang koneksi dan aktivitas pengguna di klaster Amazon Redshift, pastikan pencatatan audit diaktifkan.
1650	opensearch-audit-logging-enabled	Pastikan pencatatan audit diaktifkan di domain OpenSearch Layanan Amazon Anda. Pencatatan audit memungkinkan Anda melacak aktivitas pengguna di OpenSearch domain Anda, termasuk keberhasilan dan kegagalan otentikasi, permintaan, perubahan indeks OpenSearch, dan kueri penelusuran yang masuk.

ID Kontrol	AWS Aturan Config	Bimbingan
1650	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
1657	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1657	api-gw-associated-with-waf	AWS WAF memungkin kan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindung inya dari serangan berbahaya
1657	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1657	waf-regional-rule-not-kosong	Pastikan AWS WAF Anda memiliki aturan yang tidak kosong. Aturan tanpa kondisi dapat mengakibatkan perilaku yang tidak diinginkan.
1657	waf-regional-rulegroup-not-kosong	Pastikan AWS WAF Anda memiliki grup aturan yang tidak kosong. Grup aturan yang kosong dapat mengakiba tkan perilaku yang tidak diinginkan.
1657	waf-regional-webacl-not-kos ong	Web ACL yang dilampirk an ke AWS WAF dapat berisi kumpulan aturan dan kelompok aturan untuk memeriksa dan mengontro l permintaan web. Jika ACL Web kosong, lalu lintas web lewat tanpa terdeteksi atau ditindaklanjuti oleh WAF.

ID Kontrol	AWS Aturan Config	Bimbingan
1657	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapka n status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigura si aplikasi, dan detail lainnya tentang lingkungan Anda.
1661	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatc h untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaa n AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	AWS Aturan Config	Bimbingan
1661	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penol akan dengan merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilka n, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	AWS Aturan Config	Bimbingan
1661	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimk an file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
1661	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktif an beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.
1661	elasticsearch-logs-to-cloud watch	Pastikan domain OpenSearc h Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersediaan.
1661	api-gw-execution-logging-di aktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
1661	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
1661	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	AWS Aturan Config	Bimbingan
1661	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1661	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.
1661	vpc-flow-logs-enabled	Log aliran VPC menyediak an catatan terperinci untuk informasi tentang lalu lintas IP yang pergi ke dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	AWS Aturan Config	Bimbingan
1661	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
1661	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	AWS Aturan Config	Bimbingan
1661	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
1679	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	AWS Aturan Config	Bimbingan
1679	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
1679	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahk an lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
1679	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
1679	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
1680	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.
1680	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
1680	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahk an lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
1680	root-account-hardware-mfa-d iaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
1680	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifka n untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
1681	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	AWS Aturan Config	Bimbingan
1681	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
1681	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahk an lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
1681	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
1681	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
1683	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penol akan dengan merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilka n, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
1683	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	AWS Aturan Config	Bimbingan
1690	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunak an kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.
1690	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1690	ecs-fargate-latest-platform-versi	Pembaruan dan tambalan keamanan diterapkan secara otomatis untuk tugas Fargate AWS Anda. Jika ditemukan masalah keamanan yang memengaruhi versi platform AWS Fargate, AWS tambal versi platform. Untuk membantu pengelolaan tambalan tugas Amazon Elastic Container Service (ECS) yang menjalankan AWS Fargate, perbarui tugas mandiri layanan Anda untuk menggunakan versi platform terbaru.
1690	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	AWS Aturan Config	Bimbingan
1690	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relationa l Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.
1690	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapka n status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigura si aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1690	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automated SnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1691	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunak an kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.
1691	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1691	ecs-fargate-latest-platform-versi	Pembaruan dan tambalan keamanan diterapkan secara otomatis untuk tugas Fargate AWS Anda. Jika ditemukan masalah keamanan yang memengaruhi versi platform AWS Fargate, AWS tambal versi platform. Untuk membantu pengelolaan tambalan tugas Amazon Elastic Container Service (ECS) yang menjalankan AWS Fargate, perbarui tugas mandiri layanan Anda untuk menggunakan versi platform terbaru.
1691	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	AWS Aturan Config	Bimbingan
1691	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relationa l Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.
1691	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapka n status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigura si aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1691	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1693	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunak an kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.
1693	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1693	ecs-fargate-latest-platform-versi	Pembaruan dan tambalan keamanan diterapkan secara otomatis untuk tugas Fargate AWS Anda. Jika ditemukan masalah keamanan yang memengaruhi versi platform AWS Fargate, AWS tambal versi platform. Untuk membantu pengelolaan tambalan tugas Amazon Elastic Container Service (ECS) yang menjalankan AWS Fargate, perbarui tugas mandiri layanan Anda untuk menggunakan versi platform terbaru.
1693	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	AWS Aturan Config	Bimbingan
1693	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relationa l Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.
1693	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapka n status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigura si aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1693	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00 -sat: 16:30), dan automated SnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
1694	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1695	ec2- -periksa managedin stance-patch-compliance-sta tus	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
1707	backup-recovery-point-manua l-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	AWS Aturan Config	Bimbingan
P1	rds-cluster-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktif kan perlindungan penghapus an. Gunakan perlindun gan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya , yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
P1	rds-instance-deletion-prote ction-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktif kan perlindungan penghapus an. Gunakan perlindun gan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya , yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
P3	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunak an kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.
P5	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	AWS Aturan Config	Bimbingan
P7	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
P7	s3- bucket-ssl-requests-only	Untuk membantu melindung i data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerluka n permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
P7	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
P7	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
P8	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.
P9	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
P9	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.
P9	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
P9	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	AWS Aturan Config	Bimbingan
P9	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
P9	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.
P9	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
P9	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
P9	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
P9	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
P9	elasticache-redis-cluster-a utomatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCac he membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentuka n oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	AWS Aturan Config	Bimbingan
P9	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
P9	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relational Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
P9	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.
P10	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabun gkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
P10	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	AWS Aturan Config	Bimbingan
P10	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabun gkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandun g tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkin kan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda

ID Kontrol	AWS Aturan Config	Bimbingan
P10	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizink an tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi, pengembalian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedAc tionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
P10	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
P11	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk ACSC ISM.

Praktik Terbaik Operasional untuk AI dan ML

Paket kesesuaian ini berisi AWS Config aturan berdasarkan AI dan ML. Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Operasional untuk AI dan ML.

Praktik Terbaik Operasional untuk Amazon API Gateway

Paket kesesuaian ini berisi AWS Config aturan berdasarkan penggunaan Amazon API Gateway di dalamnya. AWS Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Amazon API Gateway.

Praktik Terbaik Operasional untuk Amazon CloudWatch

Paket kesesuaian ini berisi AWS Config aturan berdasarkan penggunaan Amazon di dalamnya. CloudWatch AWS Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Amazon CloudWatch.

Praktik Terbaik Operasional untuk Amazon DynamoDB

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Amazon DynamoDB.

Praktik Terbaik Operasional untuk Amazon S3

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Amazon S3.

Praktik Terbaik Operasional untuk APRA CPG 234

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk

membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara Australian Prudential Regulation Authority (APRA) CPG 234 dan aturan Config terkelola. AWS Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau lebih kontrol APRA CPG 234. Kontrol APRA CPG 234 dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

Templat paket kesesuaian sampel ini berisi pemetaan ke kontrol dalam APRA CPG 234 2019, yang dibuat oleh Persemakmuran Australia dan dapat ditemukan di Panduan Praktik Prudential: CPG 234 Keamanan Informasi. Lisensi kerangka kerja di bawah Lisensi Creative Commons Australia Attribution 3.0 dan informasi hak cipta untuk kerangka kerja (termasuk penafian jaminan) dapat ditemukan di APRA | Hak Cipta.

ID Kontrol	AWS Aturan Config	Bimbingan
36a	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.
36a	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi

ID Kontrol	AWS Aturan Config	Bimbingan
		dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.
36a	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
36b	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.
36b	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapka n status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigura si aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
36b	ec2- -periksa managedin stance-patch-compliance-sta tus	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
36b	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktif an beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	AWS Aturan Config	Bimbingan
36b	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00 -sat: 16:30), dan automated SnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
36b	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	AWS Aturan Config	Bimbingan
36b	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relationa l Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.
36c	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabun gkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
36c	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.
36c	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	AWS Aturan Config	Bimbingan
36c	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,338 9,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
36c	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.
36c	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	AWS Aturan Config	Bimbingan
36c	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.
36c	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
36c	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	AWS Aturan Config	Bimbingan
36d	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
36d	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
36d	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
36d	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearc h Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
36d	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
36d	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	AWS Aturan Config	Bimbingan
36d	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkin kan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabk an akses tidak sah ke sumber daya VPC Amazon.
36d	lambda-function-public-acce ss-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	AWS Aturan Config	Bimbingan
36d	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyarat an untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.
36d	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
36d	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
36d	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
36d	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	AWS Aturan Config	Bimbingan
36d	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
36d	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
36d	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaima na ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
36d	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribus i kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertah ankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	AWS Aturan Config	Bimbingan
36d	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
36d	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
36d	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.
36d	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
36d	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
36d	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurang i peluang bagi identitas untuk menerima atau mempertah ankan hak istimewa yang berlebihan.

ID Kontrol	AWS Aturan Config	Bimbingan
36d	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentif ikasi, Anda harus menonakti fkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
36d	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
36d	root-account-hardware-mfa-d iaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
36d	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifka n untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
36d	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunak an kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	AWS Aturan Config	Bimbingan
36d	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	AWS Aturan Config	Bimbingan
36d	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabun gkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandun g tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkin kan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda

ID Kontrol	AWS Aturan Config	Bimbingan
36d	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizink an tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi, pengembalian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedAc tionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda.
36d	ec2- instance-profile-attached	EC2 profil instance meneruska n peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
36d	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkin kan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
36d	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.
36d	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
36d	s3- -dilarang bucket-level-publi c-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
36d	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	AWS Aturan Config	Bimbingan
36d	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
36d	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositori data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	AWS Aturan Config	Bimbingan
36d	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
36d	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspo s informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
36d	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
36e	secretsmanager-rotation-enabled-check	Aturan ini memastikan AWS rahasia Secrets Manager telah diaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan.
36e	secretsmanager-scheduled-rotation-success-periksa	Aturan ini memastikan bahwa AWS rahasia Secrets Manager telah berhasil diputar sesuai dengan jadwal rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode di mana rahasia aktif, dan berpotensi mengurangi dampak bisnis jika dikompromikan.

ID Kontrol	AWS Aturan Config	Bimbingan
36e	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
36e	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
36e	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
36e	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearc h Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
36e	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
36e	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	AWS Aturan Config	Bimbingan
36e	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkin kan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabk an akses tidak sah ke sumber daya VPC Amazon.
36e	lambda-function-public-acce ss-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	AWS Aturan Config	Bimbingan
36e	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyarat an untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.
36e	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
36e	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
36e	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
36e	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	AWS Aturan Config	Bimbingan
36e	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
36e	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
36e	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
36e	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
36e	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
36e	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	AWS Aturan Config	Bimbingan
36e	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
36e	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositori data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	AWS Aturan Config	Bimbingan
36e	api-gw-associated-with-waf	AWS WAF memungkin kan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindung inya dari serangan berbahaya

ID Kontrol	AWS Aturan Config	Bimbingan
36e	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
36e	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspo s informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
36e	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
36f	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
36f	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
36f	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
36f	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
36f	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
36f	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	AWS Aturan Config	Bimbingan
36f	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkin kan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabk an akses tidak sah ke sumber daya VPC Amazon.
36f	lambda-function-public-acce ss-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	AWS Aturan Config	Bimbingan
36f	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyarat an untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.
36f	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
36f	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
36f	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
36f	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	AWS Aturan Config	Bimbingan
36f	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
36f	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
36f	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.
36f	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
36f	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .
36f	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	AWS Aturan Config	Bimbingan
36f	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.
36f	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
36f	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	AWS Aturan Config	Bimbingan
36f	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
36f	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
36f	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositori data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.
36f	api-gw-associated-with-waf	AWS WAF memungkin kan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindung inya dari serangan berbahaya

ID Kontrol	AWS Aturan Config	Bimbingan
36f	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
36f	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspo s informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
36f	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearc h Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
36g	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	AWS Aturan Config	Bimbingan
36g	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
36g	guardduty-non-archived-find ings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan: rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighS ev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
36 jam	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
36 jam	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
36 jam	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan: rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
36 jam	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.
36 jam	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapka n status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigura si aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
36 jam	ec2- -periksa managedin stance-patch-compliance-sta tus	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
36 jam	redshift-cluster-maintenanc esettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengatura n yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrad e. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00 -sat: 16:30), dan automated SnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
36 jam	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.
36i	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	AWS Aturan Config	Bimbingan
36i	cloudwatch-alarm-action-check	Amazon CloudWatch memperingatkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
36i	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
36i	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
36i	lambda-concurrency-check	Aturan ini memastikan bahwa batas tinggi dan rendah konkurensi fungsi Lambda ditetapkan. Ini dapat membantu dalam mendasark an jumlah permintaan yang dilayani oleh fungsi Anda pada waktu tertentu.
36i	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	AWS Aturan Config	Bimbingan
36i	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.
36i	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
36i	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	AWS Aturan Config	Bimbingan
36i	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.
36i	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
36j	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
36j	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
36j	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan: rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.
36j	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
36j	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	AWS Aturan Config	Bimbingan
36j	cloudwatch-alarm-action-check	Amazon CloudWatch memperingatkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
36j	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
36j	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.
36j	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	AWS Aturan Config	Bimbingan
36j	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.
36j	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
36l	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.
36l	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	AWS Aturan Config	Bimbingan
36l	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadang an berkelanjutan dari tabel Anda selama 35 hari terakhir.
36l	elasticache-redis-cluster-a utomatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCac he membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentuka n oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	AWS Aturan Config	Bimbingan
36l	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
36l	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) menyediakan ketersediaan dan daya tahan yang ditingkatkan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
36l	rds-cluster-multi-az-diaktifkan	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) menyediakan ketersediaan dan daya tahan yang ditingkatkan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
36l	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersedi aan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.
36l	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimpleme ntasikan untuk mencapai persyaratan ketahanan . Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-S ite VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	AWS Aturan Config	Bimbingan
36l	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
36l	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
36l	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
36l	elb-cross-zone-load-menyeim bangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkat kan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	AWS Aturan Config	Bimbingan
36l	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
36l	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relational Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
36l	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.
36l	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkin kan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentif ikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.

ID Kontrol	AWS Aturan Config	Bimbingan
39 (a) (b) (d)	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
39 (a) (b) (d)	guardduty-non-archived-find ings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan: rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighS ev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
39 (a) (b) (d)	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
40	ec2- -periksa managedin stance-patch-compliance-sta tus	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
40	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00 -sat: 16:30), dan automated SnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
40	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	AWS Aturan Config	Bimbingan
40	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relationa l Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.
44a	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
44a	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
44a	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
44b	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
44b	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	AWS Aturan Config	Bimbingan
44b	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
44c	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	AWS Aturan Config	Bimbingan
44c	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
44c	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda

ID Kontrol	AWS Aturan Config	Bimbingan
44c	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizink an tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi, pengembalian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedAc tionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
45	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
45	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
45	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.
45	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
45	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurang i peluang bagi identitas untuk menerima atau mempertah ankan hak istimewa yang berlebihan.
45	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentif ikasi, Anda harus menonakti fkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
45	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
45	root-account-hardware-mfa-d iaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
45	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
45	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribus i kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertah ankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	AWS Aturan Config	Bimbingan
45	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.
45	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
45	ebs-snapshot-public-restora ble-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihka n secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
45	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
45	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
45	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
45	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	AWS Aturan Config	Bimbingan
45	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	AWS Aturan Config	Bimbingan
45	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkin kan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabk an akses tidak sah ke sumber daya VPC Amazon.
45	lambda-function-public-acce ss-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	AWS Aturan Config	Bimbingan
45	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyarat an untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.
45	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
45	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
45	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
45	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,338 9,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
45	s3- bucket-public-read-prohibit ed	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	AWS Aturan Config	Bimbingan
45	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
45	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
45	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .
45	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	AWS Aturan Config	Bimbingan
45	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.

ID Kontrol	AWS Aturan Config	Bimbingan
45	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabun gkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandun g tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkin kan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda

ID Kontrol	AWS Aturan Config	Bimbingan
45	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizink an tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi, pengembalian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedAc tionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda.
45	ec2- instance-profile-attached	EC2 profil instance meneruska n peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
45	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkin kan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
45	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
45	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	AWS Aturan Config	Bimbingan
45	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
45	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
45	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositori data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.
45	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearc h Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	AWS Aturan Config	Bimbingan
45	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
45	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspo s informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
47c	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribus i kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertah ankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	AWS Aturan Config	Bimbingan
47c	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
47c	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
47c	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.
47c	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurang i peluang bagi identitas untuk menerima atau mempertah ankan hak istimewa yang berlebihan.

ID Kontrol	AWS Aturan Config	Bimbingan
47c	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.
47c	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkin kan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
52c	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
52c	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
52c	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
52c	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
52c	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
52c	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
52c	rds-storage-encrypted	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
52c	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
52c	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
52c	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
52c	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
52c	sns-encrypted-kms	Untuk membantu melindung i data saat istirahat, pastikan topik Amazon Simple Notificat ion Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
52c	ec2- ebs-encryption-by-default	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
52c	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
52c	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
52c	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
52c	redshift-cluster-kms-enabled	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
52c	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
52d	s3- bucket-public-read-prohibit ed	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	AWS Aturan Config	Bimbingan
52d	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
52d	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
52d	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
52d	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
52d	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
52d	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	AWS Aturan Config	Bimbingan
52d	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
52d	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	AWS Aturan Config	Bimbingan
52d	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkin kan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabk an akses tidak sah ke sumber daya VPC Amazon.
52d	lambda-function-public-acce ss-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	AWS Aturan Config	Bimbingan
52d	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyarat an untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.
52d	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
52d	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
52d	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
52d	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
52d	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
52d	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
52d	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositori data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.
52d	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspo s informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
52d	s3- -dilarang bucket-level-publi c-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
52d	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearc h Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	AWS Aturan Config	Bimbingan
52d	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
52e	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
52e	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
53	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
53	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	AWS Aturan Config	Bimbingan
53	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearc h Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
53	sagemaker-notebook-no-direc t-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
53	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
53	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
53	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
53	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	AWS Aturan Config	Bimbingan
53	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
53	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	AWS Aturan Config	Bimbingan
53	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkin kan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabk an akses tidak sah ke sumber daya VPC Amazon.
53	lambda-function-public-acce ss-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	AWS Aturan Config	Bimbingan
53	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyarat an untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.
53	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
53	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
53	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
53	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
53	s3- -dilarang bucket-level-publi c-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
53	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	AWS Aturan Config	Bimbingan
53	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
53	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositori data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	AWS Aturan Config	Bimbingan
53	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
53	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspo s informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
54	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
54	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastika n sertifikat X509 dikeluark an oleh AWS ACM. Sertifika t ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
54	alb-http-to-https-pengalihan-periksa	Untuk membantu melindung i data dalam perjalanan, pastikan bahwa Applicati on Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
54	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
54	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
54	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
54	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
54	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
54	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certifica te Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
54	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
54	rds-storage-encrypted	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
54	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastika n bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberika n informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
54	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
54	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
54	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
54	s3- bucket-ssl-requests-only	Untuk membantu melindung i data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerluka n permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
54	sagemaker-endpoint-configur ation-kms-kunci-dikonfigurasi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
54	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
54	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
54	ec2- ebs-encryption-by-default	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
54	rds-snapshot-encrypted	Pastikan enkripsi diaktifka n untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
54	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
54	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
54	redshift-cluster-kms-enabled	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
54	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifika t SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	AWS Aturan Config	Bimbingan
54	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certifica te Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
55	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
55	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
67	api-gw-execution-logging-di aktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
67	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatc h untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaa n AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	AWS Aturan Config	Bimbingan
67	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penol akan dengan merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilka n, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
67	cloudtrail-s3-dataevents-di aktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	AWS Aturan Config	Bimbingan
67	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifka n. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	AWS Aturan Config	Bimbingan
67	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimk an file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
67	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.
67	vpc-flow-logs-enabled	Log aliran VPC menyediak an catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	AWS Aturan Config	Bimbingan
67	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
67	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	AWS Aturan Config	Bimbingan
67	cloudwatch-alarm-action-check	Amazon CloudWatch memperingatkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.
67	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
67	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
67	opensearch-logs-to-cloudwat ch	Pastikan domain OpenSearc h Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpan an dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
67	ec2- -periksa managedin stance-patch-compliance-sta tus	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
67	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapka n status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigura si aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
67	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
67	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
68	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
68	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	AWS Aturan Config	Bimbingan
73	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
73	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_1 (b) (h)	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribus i kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertah ankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_1 (b) (h)	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
Lampiran_1 (b) (h)	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_1 (b) (h)	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_1 (b) (h)	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentif ikasi, Anda harus menonakti fkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_1 (b) (h)	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_1 (b) (h)	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_1 (b) (h)	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizink an tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi, pengembalian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedAc tionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_1 (b) (h)	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkin kan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
Lampiran_1 (b) (h)	ec2- instance-profile-attached	EC2 profil instance meneruska n peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_1 (c)	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
Lampiran_1 (c)	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_1 (e)	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
Lampiran_1 (e)	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_1 (e)	cloudwatch-alarm-action-check	Amazon CloudWatch memperingatkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.
Lampiran_1 (e)	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_1 (e)	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
Lampiran_1 (e)	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
Lampiran_1 (e)	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_1 (e)	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_1 (e)	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimk an file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_1 (e)	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.
Lampiran_1 (e)	vpc-flow-logs-enabled	Log aliran VPC menyediak an catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_1 (e)	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
Lampiran_1 (e)	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_1 (e)	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
Lampiran_1 (e)	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
LampiranB_1	security-awareness-program-exists (pemeriksaan proses)	Membangun dan memeliharaa program kesadaran keamanan untuk organisasi Anda. Program kesadaran keamanan mendidik karyawan tentang cara melindungi organisasi mereka dari berbagai pelanggaran atau insiden keamanan.

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_4	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaima na ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_4	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribus i kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertah ankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_4	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
LampiranC_4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_4	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.
LampiranC_4	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_4	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
LampiranC_4	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurang i peluang bagi identitas untuk menerima atau mempertah ankan hak istimewa yang berlebihan.

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_4	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentif ikasi, Anda harus menonakti fkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_4	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
LampiranC_4	root-account-hardware-mfa-d iaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_4	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifka n untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
LampiranC_4	secretsmanager-rotation-ena bled-check	Aturan ini memastikan AWS rahasia Secrets Manager telah diaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotens i mengurangi dampak bisnis jika rahasia itu dikomprom ikan.

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_4	secretsmanager-scheduled-rotation-success-periksa	Aturan ini memastikan bahwa AWS rahasia Secrets Manager telah berhasil diputar sesuai dengan jadwal rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode di mana rahasia aktif, dan berpotensi mengurangi dampak bisnis jika dikompromikan.
LampiranC_4	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_4	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_4	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizink an tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi, pengembalian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedAc tionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda.
LampiranC_4	ec2- instance-profile-attached	EC2 profil instance meneruska n peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_4	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkin kan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
LampiranC_5	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_5	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
LampiranC_5	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_5	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurang i peluang bagi identitas untuk menerima atau mempertah ankan hak istimewa yang berlebihan.

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_5	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
LampiranC_6	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
LampiranC_6	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_6	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.
LampiranC_7 (c)	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.
LampiranC_7 (h)	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_7 (h)	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
LampiranC_7 (h)	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
LampiranC_7 (h)	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_7 (h)	cloudwatch-alarm-action-check	Amazon CloudWatch memperingatkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.
LampiranC_7 (h)	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_7 (h)	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_7 (h)	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimk an file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_7 (h)	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_7 (h)	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
LampiranC_7 (h)	vpc-flow-logs-enabled	Log aliran VPC menyediak an catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_7 (h)	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
LampiranC_7 (h)	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_7 (h)	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
LampiranC_7 (h)	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_7 (i)	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentif ikasi, Anda harus menonakti fkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
LampiranC_7 (j)	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_7 (j)	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
LampiranC_7 (j)	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_7 (j)	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
LampiranC_8	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
LampiranC_8	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_8	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
LampiranC_8	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
LampiranC_8	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_8	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifka n. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_8	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimk an file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_8	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.
LampiranC_8	vpc-flow-logs-enabled	Log aliran VPC menyediak an catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_8	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
LampiranC_8	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	AWS Aturan Config	Bimbingan
LampiranC_8	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
Lampiran_1	codebuild-project-envvar-awscred-periksa	Pastikan kredensyal otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild. Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_1	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredenal masuk dalam lingkungan proyek Codebuild. AWS Gunakan OAuth alih-alih token akses pribadi atau kredensi masuk untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.
Lampiran_4	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.
Lampiran_4	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_5 (d)	cmk-backing-key-rotation-di aktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.
Lampiran_1 (a) (b) (d)	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
Lampiran_1 (a) (b) (d)	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_1 (a) (b) (d)	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
Lampiran_1 (a) (b) (d)	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Lampiran_1 (a) (b) (d)	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_1 (a) (b) (d)	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
Lampiran_1 (a) (b) (d)	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
Lampiran_1 (a) (b) (d)	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
Lampiran_1 (a) (b) (d)	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_1 (a) (b) (d)	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
Lampiran_1 (a) (b) (d)	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
Lampiran_1 (a) (b) (d)	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_1 (a) (b) (d)	rds-storage-encrypted	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Lampiran_1 (a) (b) (d)	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastika n bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberika n informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_1 (a) (b) (d)	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerluka n enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Lampiran_1 (a) (b) (d)	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
Lampiran_1 (a) (b) (d)	s3- bucket-ssl-requests-only	Untuk membantu melindung i data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerluka n permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_1 (a) (b) (d)	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Lampiran_1 (a) (b) (d)	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_1 (a) (b) (d)	sns-encrypted-kms	Untuk membantu melindung i data saat istirahat, pastikan topik Amazon Simple Notificat ion Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Lampiran_1 (a) (b) (d)	ec2- ebs-encryption-by-default	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Lampiran_1 (a) (b) (d)	rds-snapshot-encrypted	Pastikan enkripsi diaktifka n untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_1 (a) (b) (d)	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Lampiran_1 (a) (b) (d)	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Lampiran_1 (a) (b) (d)	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_1 (a) (b) (d)	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifika t SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk APRA CPG 234.

Praktik Terbaik Operasional untuk Manajemen Aset

Paket kesesuaian ini berisi AWS Config aturan berdasarkan manajemen aset di dalamnya. AWS Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Manajemen Aset.

Praktik Terbaik Operasional untuk AWS Backup

Paket kesesuaian ini berisi AWS Config aturan berdasarkan di dalam. AWS Backup AWS Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Operasional untuk AWS Backup.

Praktik Terbaik Operasional untuk Manajemen AWS Identitas Dan Akses

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Manajemen AWS Identitas Dan Akses.

Praktik Terbaik Operasional untuk Pilar Keandalan AWS Kerangka Well-Architected

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini menyediakan contoh pemetaan antara Pilar Keandalan Kerangka Kerja Well-Architected Amazon Web Services dan aturan Config terkelola. AWS Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan berhubungan dengan satu atau beberapa prinsip desain pilar. Kategori Well-Architected Framework dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-1	Bagaimana Anda mengelola kuota dan kendala layanan? Untuk arsitektur beban kerja berbasis cloud, ada service quotas (kuota layanan) (yang juga disebut sebagai batas layanan). Kuota ini ada untuk mencegah penyediaan sumber daya lebih yang tidak disengaja melebihi kebutuhan Anda dan untuk membatasi tingkat permintaan di operasi API sehingga	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyarat

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	melindungi layanan dari penyalahgunaan. Ada juga kendala-k endala sumber daya, misalnya, laju Anda dapat mendorong bit di kabel serat optik, atau jumlah penyimpanan di diska secara fisik.		an throughput Anda. Aturan ini menghasil kan peringatan ketika throughpu t mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentas e WCUThreshold akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-1	Bagaimana Anda mengelola kuota dan kendala layanan? Untuk arsitektur beban kerja berbasis cloud, ada service quotas (kuota layanan) (yang juga disebut sebagai batas layanan). Kuota ini ada untuk mencegah penyediaan sumber daya lebih yang tidak disengaja melebihi kebutuhan Anda dan untuk membatasi tingkat permintaan di operasi API sehingga melindungi layanan dari penyalahgunaan. Ada juga kendala-kendala sumber daya, misalnya, laju Anda dapat mendorong bit di kabel serat optik, atau jumlah penyimpanan di diska secara fisik.	lambda-concurrency-check	Aturan ini memastikan bahwa batas tinggi dan rendah konkurensi fungsi Lambda ditetapkan. Ini dapat membantu dalam mendasarkan jumlah permintaan yang dilayani oleh fungsi Anda pada waktu tertentu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-1	Bagaimana Anda mengelola kuota dan kendala layanan? Untuk arsitektur beban kerja berbasis cloud, ada service quotas (kuota layanan) (yang juga disebut sebagai batas layanan). Kuota ini ada untuk mencegah penyediaan sumber daya lebih yang tidak disengaja melebihi kebutuhan Anda dan untuk membatasi tingkat permintaan di operasi API sehingga melindungi layanan dari penyalahgunaan. Ada juga kendala-k endala sumber daya, misalnya, laju Anda dapat mendorong bit di kabel serat optik, atau jumlah penyimpanan di diska secara fisik.	ecs-task-definition-memory-batas-keras	Membatasi memori maksimum yang tersedia untuk penampung Amazon Elastic Container Service (ECS) memastikan bahwa penggunaan sumber daya Anda tidak dapat disalahgu nakan jika terjadi akses berbahaya ke kontainer Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-2	Bagaimana cara merencanakan topologi jaringan Anda? Sering kali beban kerja ada di beberapa lingkungan. Ini termasuk beberapa lingkungan cloud (baik yang dapat diakses publik maupun privat) dan kemungkinan infrastruktur pusat data Anda yang ada sekarang. Rencana harus mencakup pertimbangan jaringan seperti konektivitas di dalam dan antarsistem, pengelolaan alamat IP publik, pengelolaan alamat IP privat, dan resolusi nama domain.	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-2	Bagaimana cara merencanakan topologi jaringan Anda? Sering kali beban kerja ada di beberapa lingkungan. Ini termasuk beberapa lingkungan cloud (baik yang dapat diakses publik maupun privat) dan kemungkinan infrastruktur pusat data Anda yang ada sekarang. Rencana harus mencakup pertimbangan jaringan seperti konektivitas di dalam dan antarsistem, pengelolaan alamat IP publik, pengelolaan alamat IP privat, dan resolusi nama domain.	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositori data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-2	Bagaimana cara merencanakan topologi jaringan Anda? Sering kali beban kerja ada di beberapa lingkungan. Ini termasuk beberapa lingkungan cloud (baik yang dapat diakses publik maupun privat) dan kemungkinan infrastruktur pusat data Anda yang ada sekarang. Rencana harus mencakup pertimbangan jaringan seperti konektivitas di dalam dan antarsist em, pengelolaan alamat IP publik, pengelolaan alamat IP privat, dan resolusi nama domain.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-5	Bagaimana Anda Merancang Interaksi dalam Sistem Terdistribusi untuk Mengurangi atau Menahan Kegagalan ? Sistem terdistri busi mengandal kan jaringan komunikasi untuk membuat interkone ksi komponen, seperti server atau layanan. Beban kerja Anda harus beroperasi secara andal terlepas latensi atau hilangnya data yang terjadi di jaringan-jaringan ini. Komponen dari sistem terdistribusi harus beroperasi dengan cara yang tidak secara negatif memengaruhi beban kerja atau komponen-komponen lain. Berbagai praktik terbaik ini mencegah kegagalan dan meningkatkan waktu rata-rata antara kegagalan (MTBF).	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-6	Bagaimana cara memantau sumber daya beban kerja Anda? Log dan metrik merupakan alat yang luar biasa untuk mendapatkan wawasan mengenai kondisi beban kerja Anda. Anda dapat mengonfigurasikan beban kerja Anda untuk memantau log dan metrik serta mengirimkan notifikasi ketika ambang batas terlampaui atau ada peristiwa signifikan yang terjadi. Pemantauan memungkinkan beban kerja Anda mengenali kapan ambang batas kinerja rendah dilintasi atau terjadi kegagalan, sehingga dapat pulih secara otomatis sebagai respons.	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-6	Bagaimana cara memantau sumber daya beban kerja Anda? Log dan metrik merupakan alat yang luar biasa untuk mendapatkan wawasan mengenai kondisi beban kerja Anda. Anda dapat mengonfigurasikan beban kerja Anda untuk memantau log dan metrik serta mengirimkan notifikasi ketika ambang batas terlampaui atau ada peristiwa signifikan yang terjadi. Pemantauan memungkinkan beban kerja Anda mengenali kapan ambang batas kinerja rendah dilintasi atau terjadi kegagalan, sehingga dapat pulih secara otomatis sebagai respons.	api-gw-xray-enabled	AWS X-Ray mengumpulkan data tentang permintaan yang disajikan aplikasi Anda, dan menyediakan alat yang dapat Anda gunakan untuk melihat, memfilter, dan mendapatkan wawasan tentang data tersebut guna mengidentifikasi masalah dan peluang pengoptimalan. Pastikan X-Ray diaktifkan sehingga Anda dapat melihat informasi terperinci tidak hanya tentang permintaan dan respons, tetapi juga tentang panggilan yang dilakukan aplikasi Anda ke AWS sumber daya hilir, layanan mikro, database, dan web HTTP. APIs

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-6	Bagaimana cara memantau sumber daya beban kerja Anda? Log dan metrik merupakan alat yang luar biasa untuk mendapatkan wawasan mengenai kondisi beban kerja Anda. Anda dapat mengonfigurasikan beban kerja Anda untuk memantau log dan metrik serta mengirimkan notifikasi ketika ambang batas terlampaui atau ada peristiwa signifikan yang terjadi. Pemantauan memungkinkan beban kerja Anda mengenali kapan ambang batas kinerja rendah dilintasi atau terjadi kegagalan, sehingga dapat pulih secara otomatis sebagai respons.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-6	Bagaimana cara memantau sumber daya beban kerja Anda? Log dan metrik merupakan alat yang luar biasa untuk mendapatkan wawasan mengenai kondisi beban kerja Anda. Anda dapat mengonfigurasikan beban kerja Anda untuk memantau log dan metrik serta mengirimkan notifikasi ketika ambang batas terlampaui atau ada peristiwa signifikan yang terjadi. Pemantauan memungkinkan beban kerja Anda mengenali kapan ambang batas kinerja rendah dilintasi atau terjadi kegagalan, sehingga dapat pulih secara otomatis sebagai respons.	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-6	Bagaimana cara memantau sumber daya beban kerja Anda? Log dan metrik merupakan alat yang luar biasa untuk mendapatkan wawasan mengenai kondisi beban kerja Anda. Anda dapat mengonfigurasikan beban kerja Anda untuk memantau log dan metrik serta mengirimkan notifikasi ketika ambang batas terlampaui atau ada peristiwa signifikan yang terjadi. Pemantauan memungkinkan beban kerja Anda mengenali kapan ambang batas kinerja rendah dilintasi atau terjadi kegagalan, sehingga dapat pulih secara otomatis sebagai respons.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-6	Bagaimana cara memantau sumber daya beban kerja Anda? Log dan metrik merupakan alat yang luar biasa untuk mendapatkan wawasan mengenai kondisi beban kerja Anda. Anda dapat mengonfigurasikan beban kerja Anda untuk memantau log dan metrik serta mengirimkan notifikasi ketika ambang batas terlampaui atau ada peristiwa signifikan yang terjadi. Pemantauan memungkinkan beban kerja Anda mengenali kapan ambang batas kinerja rendah dilintasi atau terjadi kegagalan, sehingga dapat pulih secara otomatis sebagai respons.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-6	Bagaimana cara memantau sumber daya beban kerja Anda? Log dan metrik merupakan alat yang luar biasa untuk mendapatkan wawasan mengenai kondisi beban kerja Anda. Anda dapat mengonfigurasikan beban kerja Anda untuk memantau log dan metrik serta mengirimkan notifikasi ketika ambang batas terlampaui atau ada peristiwa signifikan yang terjadi. Pemantauan memungkinkan beban kerja Anda mengenali kapan ambang batas kinerja rendah dilintasi atau terjadi kegagalan, sehingga dapat pulih secara otomatis sebagai respons.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-6	Bagaimana cara memantau sumber daya beban kerja Anda? Log dan metrik merupakan alat yang luar biasa untuk mendapatkan wawasan mengenai kondisi beban kerja Anda. Anda dapat mengonfigurasikan beban kerja Anda untuk memantau log dan metrik serta mengirimkan notifikasi ketika ambang batas terlampaui atau ada peristiwa signifikan yang terjadi. Pemantauan memungkinkan beban kerja Anda mengenali kapan ambang batas kinerja rendah dilintasi atau terjadi kegagalan, sehingga dapat pulih secara otomatis sebagai respons.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-6	Bagaimana cara memantau sumber daya beban kerja Anda? Log dan metrik merupakan alat yang luar biasa untuk mendapatkan wawasan mengenai kondisi beban kerja Anda. Anda dapat mengonfigurasikan beban kerja Anda untuk memantau log dan metrik serta mengirimkan notifikasi ketika ambang batas terlampaui atau ada peristiwa signifikan yang terjadi. Pemantauan memungkinkan beban kerja Anda mengenali kapan ambang batas kinerja rendah dilintasi atau terjadi kegagalan, sehingga dapat pulih secara otomatis sebagai respons.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-6	Bagaimana cara memantau sumber daya beban kerja Anda? Log dan metrik merupakan alat yang luar biasa untuk mendapatkan wawasan mengenai kondisi beban kerja Anda. Anda dapat mengonfigurasikan beban kerja Anda untuk memantau log dan metrik serta mengirimkan notifikasi ketika ambang batas terlampaui atau ada peristiwa signifikan yang terjadi. Pemantauan memungkinkan beban kerja Anda mengenali kapan ambang batas kinerja rendah dilintasi atau terjadi kegagalan, sehingga dapat pulih secara otomatis sebagai respons.	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-6	Bagaimana cara memantau sumber daya beban kerja Anda? Log dan metrik merupakan alat yang luar biasa untuk mendapatkan wawasan mengenai kondisi beban kerja Anda. Anda dapat mengonfigurasikan beban kerja Anda untuk memantau log dan metrik serta mengirimkan notifikasi ketika ambang batas terlampaui atau ada peristiwa signifikan yang terjadi. Pemantauan memungkinkan beban kerja Anda mengenali kapan ambang batas kinerja rendah dilintasi atau terjadi kegagalan, sehingga dapat pulih secara otomatis sebagai respons.	ecs-container-insights-enabled	Pemantauan merupakan bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja Amazon Elastic Container Service (ECS) dan AWS solusi Anda. Wawasan Kontainer juga akan menyediakan informasi diagnostik, seperti kegagalan mengulang kembali kontainer, untuk membantu Anda melakukan isolasi atas masalah dan mengatasi masalah itu dengan cepat.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-6	Bagaimana cara memantau sumber daya beban kerja Anda? Log dan metrik merupakan alat yang luar biasa untuk mendapatkan wawasan mengenai kondisi beban kerja Anda. Anda dapat mengonfigurasikan beban kerja Anda untuk memantau log dan metrik serta mengirimkan notifikasi ketika ambang batas terlampaui atau ada peristiwa signifikan yang terjadi. Pemantauan memungkinkan beban kerja Anda mengenali kapan ambang batas kinerja rendah dilintasi atau terjadi kegagalan, sehingga dapat pulih secara otomatis sebagai respons.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-6	Bagaimana cara memantau sumber daya beban kerja Anda? Log dan metrik merupakan alat yang luar biasa untuk mendapatkan wawasan mengenai kondisi beban kerja Anda. Anda dapat mengonfigurasikan beban kerja Anda untuk memantau log dan metrik serta mengirimkan notifikasi ketika ambang batas terlampaui atau ada peristiwa signifikan yang terjadi. Pemantauan memungkinkan beban kerja Anda mengenali kapan ambang batas kinerja rendah dilintasi atau terjadi kegagalan, sehingga dapat pulih secara otomatis sebagai respons.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-6	Bagaimana cara memantau sumber daya beban kerja Anda? Log dan metrik merupakan alat yang luar biasa untuk mendapatkan wawasan mengenai kondisi beban kerja Anda. Anda dapat mengonfigurasikan beban kerja Anda untuk memantau log dan metrik serta mengirimkan notifikasi ketika ambang batas terlampaui atau ada peristiwa signifikan yang terjadi. Pemantauan memungkinkan beban kerja Anda mengenali kapan ambang batas kinerja rendah dilintasi atau terjadi kegagalan, sehingga dapat pulih secara otomatis sebagai respons.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-6	Bagaimana cara memantau sumber daya beban kerja Anda? Log dan metrik merupakan alat yang luar biasa untuk mendapatkan wawasan mengenai kondisi beban kerja Anda. Anda dapat mengonfigurasikan beban kerja Anda untuk memantau log dan metrik serta mengirimkan notifikasi ketika ambang batas terlampaui atau ada peristiwa signifikan yang terjadi. Pemantauan memungkinkan beban kerja Anda mengenali kapan ambang batas kinerja rendah dilintasi atau terjadi kegagalan, sehingga dapat pulih secara otomatis sebagai respons.	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-6	Bagaimana cara memantau sumber daya beban kerja Anda? Log dan metrik merupakan alat yang luar biasa untuk mendapatkan wawasan mengenai kondisi beban kerja Anda. Anda dapat mengonfigurasikan beban kerja Anda untuk memantau log dan metrik serta mengirimkan notifikasi ketika ambang batas terlampaui atau ada peristiwa signifikan yang terjadi. Pemantauan memungkinkan beban kerja Anda mengenali kapan ambang batas kinerja rendah dilintasi atau terjadi kegagalan, sehingga dapat pulih secara otomatis sebagai respons.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-6	Bagaimana cara memantau sumber daya beban kerja Anda? Log dan metrik merupakan alat yang luar biasa untuk mendapatkan wawasan mengenai kondisi beban kerja Anda. Anda dapat mengonfigurasikan beban kerja Anda untuk memantau log dan metrik serta mengirimkan notifikasi ketika ambang batas terlampaui atau ada peristiwa signifikan yang terjadi. Pemantauan memungkinkan beban kerja Anda mengenali kapan ambang batas kinerja rendah dilintasi atau terjadi kegagalan, sehingga dapat pulih secara otomatis sebagai respons.	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-6	Bagaimana cara memantau sumber daya beban kerja Anda? Log dan metrik merupakan alat yang luar biasa untuk mendapatkan wawasan mengenai kondisi beban kerja Anda. Anda dapat mengonfigurasikan beban kerja Anda untuk memantau log dan metrik serta mengirimkan notifikasi ketika ambang batas terlampaui atau ada peristiwa signifikan yang terjadi. Pemantauan memungkinkan beban kerja Anda mengenali kapan ambang batas kinerja rendah dilintasi atau terjadi kegagalan, sehingga dapat pulih secara otomatis sebagai respons.	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-6	Bagaimana cara memantau sumber daya beban kerja Anda? Log dan metrik merupakan alat yang luar biasa untuk mendapatkan wawasan mengenai kondisi beban kerja Anda. Anda dapat mengonfigurasikan beban kerja Anda untuk memantau log dan metrik serta mengirimkan notifikasi ketika ambang batas terlampaui atau ada peristiwa signifikan yang terjadi. Pemantauan memungkinkan beban kerja Anda mengenali kapan ambang batas kinerja rendah dilintasi atau terjadi kegagalan, sehingga dapat pulih secara otomatis sebagai respons.	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositori data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-6	Bagaimana cara memantau sumber daya beban kerja Anda? Log dan metrik merupakan alat yang luar biasa untuk mendapatkan wawasan mengenai kondisi beban kerja Anda. Anda dapat mengonfigurasikan beban kerja Anda untuk memantau log dan metrik serta mengirimkan notifikasi ketika ambang batas terlampaui atau ada peristiwa signifikan yang terjadi. Pemantauan memungkinkan beban kerja Anda mengenali kapan ambang batas kinerja rendah dilintasi atau terjadi kegagalan, sehingga dapat pulih secara otomatis sebagai respons.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-6	Bagaimana cara memantau sumber daya beban kerja Anda? Log dan metrik merupakan alat yang luar biasa untuk mendapatkan wawasan mengenai kondisi beban kerja Anda. Anda dapat mengonfigurasikan beban kerja Anda untuk memantau log dan metrik serta mengirimkan notifikasi ketika ambang batas terlampaui atau ada peristiwa signifikan yang terjadi. Pemantauan memungkinkan beban kerja Anda mengenali kapan ambang batas kinerja rendah dilintasi atau terjadi kegagalan, sehingga dapat pulih secara otomatis sebagai respons.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-6	Bagaimana cara memantau sumber daya beban kerja Anda? Log dan metrik merupakan alat yang luar biasa untuk mendapatkan wawasan mengenai kondisi beban kerja Anda. Anda dapat mengonfigurasikan beban kerja Anda untuk memantau log dan metrik serta mengirimkan notifikasi ketika ambang batas terlampaui atau ada peristiwa signifikan yang terjadi. Pemantauan memungkinkan beban kerja Anda mengenali kapan ambang batas kinerja rendah dilintasi atau terjadi kegagalan, sehingga dapat pulih secara otomatis sebagai respons.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-6	Bagaimana cara memantau sumber daya beban kerja Anda? Log dan metrik merupakan alat yang luar biasa untuk mendapatkan wawasan mengenai kondisi beban kerja Anda. Anda dapat mengonfigurasikan beban kerja Anda untuk memantau log dan metrik serta mengirimkan notifikasi ketika ambang batas terlampaui atau ada peristiwa signifikan yang terjadi. Pemantauan memungkinkan beban kerja Anda mengenali kapan ambang batas kinerja rendah dilintasi atau terjadi kegagalan, sehingga dapat pulih secara otomatis sebagai respons.	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-7	Bagaimana cara mendesain beban kerja Anda untuk beradaptasi dengan perubahan dalam permintaan? Beban kerja yang dapat diskalakan memberikan elastisitas untuk menambahkan atau mengeluarkan sumber daya secara otomatis sehingga sangat sesuai dengan permintaan saat ini pada titik waktu tertentu.	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-7	Bagaimana cara mendesain beban kerja Anda untuk beradaptasi dengan perubahan dalam permintaan? Beban kerja yang dapat diskalakan memberikan elastisitas untuk menambahkan atau mengeluarkan sumber daya secara otomatis sehingga sangat sesuai dengan permintaan saat ini pada titik waktu tertentu.	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-7	Bagaimana cara mendesain beban kerja Anda untuk beradaptasi dengan perubahan dalam permintaan? Beban kerja yang dapat diskalakan memberikan elastisitas untuk menambahkan atau mengeluarkan sumber daya secara otomatis sehingga sangat sesuai dengan permintaan saat ini pada titik waktu tertentu.	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-8	Bagaimana cara mengimplementasikan perubahan? Perubahan terkontrol diperlukan untuk menyebarkan fungsionalitas baru, dan untuk memastikan bahwa beban kerja dan lingkungan operasi menjalankan perangkat lunak yang dikenal dan dapat ditambal atau diganti dengan cara yang dapat diprediksi. Jika perubahan-perubahan ini tidak terkontrol, maka akan sulit untuk memprediksi efek dari perubahan-perubahan tersebut, atau untuk mengatasi masalah yang timbul sebagai akibatnya.	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-8	Bagaimana cara mengimplementasikan perubahan? Perubahan terkontrol diperlukan untuk menyebarkan fungsionalitas baru, dan untuk memastikan bahwa beban kerja dan lingkungan operasi menjalankan perangkat lunak yang dikenal dan dapat ditambal atau diganti dengan cara yang dapat diprediksi. Jika perubahan-perubahan ini tidak terkontrol, maka akan sulit untuk memprediksi efek dari perubahan-perubahan tersebut, atau untuk mengatasi masalah yang timbul sebagai akibatnya.	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relational Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-8	Bagaimana cara mengimplementasikan perubahan? Perubahan terkontrol diperlukan untuk menyebarkan fungsionalitas baru, dan untuk memastikan bahwa beban kerja dan lingkungan operasi menjalankan perangkat lunak yang dikenal dan dapat ditambal atau diganti dengan cara yang dapat diprediksi. Jika perubahan-perubahan ini tidak terkontrol, maka akan sulit untuk memprediksi efek dari perubahan-perubahan tersebut, atau untuk mengatasi masalah yang timbul sebagai akibatnya.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-8	Bagaimana cara mengimplementasikan perubahan? Perubahan terkontrol diperlukan untuk menyebarkan fungsionalitas baru, dan untuk memastikan bahwa beban kerja dan lingkungan operasi menjalankan perangkat lunak yang dikenal dan dapat ditambal atau diganti dengan cara yang dapat diprediksi. Jika perubahan-perubahan ini tidak terkontrol, maka akan sulit untuk memprediksi efek dari perubahan-perubahan tersebut, atau untuk mengatasi masalah yang timbul sebagai akibatnya.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigurasi untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigurasi untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigurasi untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigurasi untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigurasi untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigurasi untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigurasi untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigurasi untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigura si untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigura si untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigura si untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigurasi untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigurasi untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigurasi untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigura si untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigurasi untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigurasi untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigura si untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigurasi untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigurasi untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigurasi untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigurasi untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigurasi untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigurasi untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigurasi untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigurasi untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigurasi untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigura si untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-9	Bagaimana cara mencadangkan data? Cadangkan data, aplikasi, dan konfigura si untuk memenuhi persyaratan Anda untuk sasaran waktu pemulihan (RTO) dan sasaran titik pemulihan (RPO).	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-10	Bagaimana cara menggunakan isolasi kesalahan untuk melindungi beban kerja? Batas isolasi kesalahan membatasi efek dari sebuah kegagalan di dalam beban kerja hingga jumlah komponen yang terbatas. Komponen-komponen yang ada di luar batasan-batasan ini tidak terpengaruh oleh kegagalan tersebut. Menggunakan beberapa batasan isolasi kesalahan, Anda dapat membatasi dampak pada beban kerja Anda.	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-10	Bagaimana cara menggunakan isolasi kesalahan untuk melindungi beban kerja? Batas isolasi kesalahan membatasi efek dari sebuah kegagalan di dalam beban kerja hingga jumlah komponen yang terbatas. Komponen-komponen yang ada di luar batasan-batasan ini tidak terpengaruh oleh kegagalan tersebut. Menggunakan beberapa batasan isolasi kesalahan, Anda dapat membatasi dampak pada beban kerja Anda.	clb-multiple-az	Elastic Load Balancing (ELB) secara otomatis mendistribusikan lalu lintas masuk Anda di beberapa target, seperti EC2 instance, kontainer, dan alamat IP, di zona ketersediaan. Untuk memastikan ketersediaan tinggi, pastikan ELB Anda telah mendaftarkan instans dari beberapa Availability Zone.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-10	Bagaimana cara menggunakan isolasi kesalahan untuk melindungi beban kerja? Batas isolasi kesalahan membatasi efek dari sebuah kegagalan di dalam beban kerja hingga jumlah komponen yang terbatas. Komponen-komponen yang ada di luar batasan-batasan ini tidak terpengaruh oleh kegagalan tersebut. Menggunakan beberapa batasan isolasi kesalahan, Anda dapat membatasi dampak pada beban kerja Anda.	elbv2-multiple-az	Elastic Load Balancing (ELB) secara otomatis mendistribusikan lalu lintas masuk Anda di beberapa target, seperti EC2 instance, kontainer, dan alamat IP, di zona ketersediaan. Untuk memastikan ketersediaan tinggi, pastikan ELB Anda telah mendaftarkan instans dari beberapa Availability Zone.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-10	Bagaimana cara menggunakan isolasi kesalahan untuk melindungi beban kerja? Batas isolasi kesalahan membatasi efek dari sebuah kegagalan di dalam beban kerja hingga jumlah komponen yang terbatas. Komponen-komponen yang ada di luar batasan-batasan ini tidak terpengar uh oleh kegagalan tersebut. Menggunak an beberapa batasan isolasi kesalahan , Anda dapat membatasi dampak pada beban kerja Anda.	lambda-vpc-multi-az-periksa	Jika fungsi AWS Lambda Anda dikonfigurasi untuk terhubung ke virtual private cloud (VPC) di akun Anda, gunakan fungsi AWS Lambda di setidaknya dua Availability Zone yang berbeda untuk memastikan bahwa fungsi Anda tersedia untuk memproses peristiwa jika terjadi gangguan layanan di satu zona.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-10	Bagaimana cara menggunakan isolasi kesalahan untuk melindungi beban kerja? Batas isolasi kesalahan membatasi efek dari sebuah kegagalan di dalam beban kerja hingga jumlah komponen yang terbatas. Komponen-komponen yang ada di luar batasan-batasan ini tidak terpengaruh oleh kegagalan tersebut. Menggunakan beberapa batasan isolasi kesalahan, Anda dapat membatasi dampak pada beban kerja Anda.	opensearch-data-node-fault-toleransi	Amazon OpenSearch Service (OpenSearch Service) memerlukan setidaknya tiga node data untuk ketersediaan tinggi dan toleransi kesalahan. Menyebarkan domain OpenSearch Layanan dengan setidaknya tiga node data memastikan operasi klaster jika node gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-10	Bagaimana cara menggunakan isolasi kesalahan untuk melindungi beban kerja? Batas isolasi kesalahan membatasi efek dari sebuah kegagalan di dalam beban kerja hingga jumlah komponen yang terbatas. Komponen-komponen yang ada di luar batasan-batasan ini tidak terpengaruh oleh kegagalan tersebut. Menggunakan beberapa batasan isolasi kesalahan, Anda dapat membatasi dampak pada beban kerja Anda.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-10	Bagaimana cara menggunakan isolasi kesalahan untuk melindungi beban kerja? Batas isolasi kesalahan membatasi efek dari sebuah kegagalan di dalam beban kerja hingga jumlah komponen yang terbatas. Komponen-komponen yang ada di luar batasan-batasan ini tidak terpengaruh oleh kegagalan tersebut. Menggunakan beberapa batasan isolasi kesalahan, Anda dapat membatasi dampak pada beban kerja Anda.	rds-cluster-multi-az-diaktifkan	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
REL-10	Bagaimana cara menggunakan isolasi kesalahan untuk melindungi beban kerja? Batas isolasi kesalahan membatasi efek dari sebuah kegagalan di dalam beban kerja hingga jumlah komponen yang terbatas. Komponen-komponen yang ada di luar batasan-batasan ini tidak terpengaruh oleh kegagalan tersebut. Menggunakan beberapa batasan isolasi kesalahan, Anda dapat membatasi dampak pada beban kerja Anda.	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Pilar Keandalan AWS yang Dirancang dengan Baik.

Praktik Terbaik Operasional untuk Pilar Keamanan AWS Kerangka Well-Architected

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini menyediakan contoh pemetaan antara Pilar Keamanan Well-Architected Framework Amazon Web Services dan aturan Config terkelola. AWS Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan berhubungan dengan satu atau beberapa prinsip desain pilar. Kategori Well-Architected Framework dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 1	Bagaimana cara Anda mengoperasikan beban kerja Anda dengan aman? Untuk mengoperasikan beban kerja dengan aman, Anda harus menerapkan praktik terbaik yang menyeluruh ke setiap area keamanan. Pilih persyaratan dan proses yang telah Anda tetapkan dalam keunggulan operasional di tingkat organisasi dan beban kerja, lalu terapkan	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	ke semua area. Tetap up to date dengan rekomendasi industri AWS dan intelijen ancaman membantu Anda mengemban gkan model ancaman dan tujuan pengendalian Anda. Otomatisasi proses, pengujian, dan validasi keamanan memungkinkan Anda menskalakan operasi keamanan Anda.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 1	Bagaimana cara Anda mengopera sikan beban kerja Anda dengan aman? Untuk mengopera sikan beban kerja dengan aman, Anda harus menerapkan praktik terbaik yang menyeluruh ke setiap area keamanan. Pilih persyaratan dan proses yang telah Anda tetapkan dalam keunggulan operasional di tingkat organisasi dan beban kerja, lalu terapkan ke semua area. Tetap up to date dengan rekomendasi industri AWS dan intelijen ancaman membantu Anda mengemban gkan model ancaman dan tujuan pengendalian Anda. Otomatisasi proses, pengujian, dan validasi keamanan memungkinkan Anda menskalakan operasi keamanan Anda.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 1	Bagaimana cara Anda mengopera sikan beban kerja Anda dengan aman? Untuk mengopera sikan beban kerja dengan aman, Anda harus menerapkan praktik terbaik yang menyeluruh ke setiap area keamanan. Pilih persyaratan dan proses yang telah Anda tetapkan dalam keunggulan operasional di tingkat organisasi dan beban kerja, lalu terapkan ke semua area. Tetap up to date dengan rekomendasi industri AWS dan intelijen ancaman membantu Anda mengemban gkan model ancaman dan tujuan pengendalian Anda. Otomatisasi proses, pengujian, dan validasi keamanan memungkinkan Anda menskalakan operasi keamanan Anda.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastika n otentikasi multi-fak tor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 1	Bagaimana cara Anda mengopera sikan beban kerja Anda dengan aman? Untuk mengopera sikan beban kerja dengan aman, Anda harus menerapkan praktik terbaik yang menyeluruh ke setiap area keamanan. Pilih persyaratan dan proses yang telah Anda tetapkan dalam keunggulan operasional di tingkat organisasi dan beban kerja, lalu terapkan ke semua area. Tetap up to date dengan rekomendasi industri AWS dan intelijen ancaman membantu Anda mengemban gkan model ancaman dan tujuan pengendalian Anda. Otomatisasi proses, pengujian, dan validasi keamanan memungkinkan Anda menskalakan operasi keamanan Anda.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 1	Bagaimana cara Anda mengopera sikan beban kerja Anda dengan aman? Untuk mengopera sikan beban kerja dengan aman, Anda harus menerapkan praktik terbaik yang menyeluruh ke setiap area keamanan. Pilih persyaratan dan proses yang telah Anda tetapkan dalam keunggulan operasional di tingkat organisasi dan beban kerja, lalu terapkan ke semua area. Tetap up to date dengan rekomendasi industri AWS dan intelijen ancaman membantu Anda mengemban gkan model ancaman dan tujuan pengendalian Anda. Otomatisasi proses, pengujian, dan validasi keamanan memungkinkan Anda menskalakan operasi keamanan Anda.	root-account-hardw are-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindun gan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 1	Bagaimana cara Anda mengoperasikan beban kerja Anda dengan aman? Untuk mengoperasikan beban kerja dengan aman, Anda harus menerapkan praktik terbaik yang menyeluruh ke setiap area keamanan. Pilih persyaratan dan proses yang telah Anda tetapkan dalam keunggulan operasional di tingkat organisasi dan beban kerja, lalu terapkan ke semua area. Tetap up to date dengan rekomendasi industri AWS dan intelijen ancaman membantu Anda mengembangkan model ancaman dan tujuan pengendalian Anda. Otomatisasi proses, pengujian, dan validasi keamanan memungkinkan Anda menskalakan operasi keamanan Anda.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 1	Bagaimana cara Anda mengopera sikan beban kerja Anda dengan aman? Untuk mengopera sikan beban kerja dengan aman, Anda harus menerapkan praktik terbaik yang menyeluruh ke setiap area keamanan. Pilih persyaratan dan proses yang telah Anda tetapkan dalam keunggulan operasional di tingkat organisasi dan beban kerja, lalu terapkan ke semua area. Tetap up to date dengan rekomendasi industri AWS dan intelijen ancaman membantu Anda mengemban gkan model ancaman dan tujuan pengendalian Anda. Otomatisasi proses, pengujian, dan validasi keamanan memungkinkan Anda menskalakan operasi keamanan Anda.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 1	Bagaimana cara Anda mengoperasikan beban kerja Anda dengan aman? Untuk mengoperasikan beban kerja dengan aman, Anda harus menerapkan praktik terbaik yang menyeluruh ke setiap area keamanan. Pilih persyaratan dan proses yang telah Anda tetapkan dalam keunggulan operasional di tingkat organisasi dan beban kerja, lalu terapkan ke semua area. Tetap up to date dengan rekomendasi industri AWS dan intelijen ancaman membantu Anda mengembangkan model ancaman dan tujuan pengendalian Anda. Otomatisasi proses, pengujian, dan validasi keamanan memungkinkan Anda menskalakan operasi keamanan Anda.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi ke instans terkelola Anda dan memungkinkan Anda untuk menetapkan garis dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 1	Bagaimana cara Anda mengoperasikan beban kerja Anda dengan aman? Untuk mengoperasikan beban kerja dengan aman, Anda harus menerapkan praktik terbaik yang menyeluruh ke setiap area keamanan. Pilih persyaratan dan proses yang telah Anda tetapkan dalam keunggulan operasional di tingkat organisasi dan beban kerja, lalu terapkan ke semua area. Tetap up to date dengan rekomendasi industri AWS dan intelijen ancaman membantu Anda mengembangkan model ancaman dan tujuan pengendalian Anda. Otomatisasi proses, pengujian, dan validasi keamanan memungkinkan Anda menskalakan operasi keamanan Anda.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 1	Bagaimana cara Anda mengoperasikan beban kerja Anda dengan aman? Untuk mengoperasikan beban kerja dengan aman, Anda harus menerapkan praktik terbaik yang menyeluruh ke setiap area keamanan. Pilih persyaratan dan proses yang telah Anda tetapkan dalam keunggulan operasional di tingkat organisasi dan beban kerja, lalu terapkan ke semua area. Tetap up to date dengan rekomendasi industri AWS dan intelijen ancaman membantu Anda mengembangkan model ancaman dan tujuan pengendalian Anda. Otomatisasi proses, pengujian, dan validasi keamanan memungkinkan Anda menskalakan operasi keamanan Anda.	codebuild-project-envvar-awscred-periksa	Pastikan kredensial otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild. Jangan menyimpan variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 2	Bagaimana Anda mengelola identitas untuk orang dan mesin? Ada dua jenis identitas yang perlu Anda kelola saat mendekati beban AWS kerja yang aman. Memahami jenis identitas yang Anda butuhkan untuk mengelola dan memberikan akses membantu Anda memastikan identitas yang tepat memiliki akses ke sumber daya yang tepat dalam kondisi yang tepat. Identitas Manusia: Administrator, pengembang, operator, dan pengguna akhir Anda memerlukan identitas untuk mengakses AWS lingkungan dan aplikasi Anda. Ini adalah anggota organisasi Anda, atau pengguna eksternal dengan siapa Anda berkolaborasi, dan yang berinteraksi	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dengan AWS sumber daya Anda dari browser web, aplikasi klien, atau alat baris perintah interakti f. Identitas Mesin: Aplikasi layanan, alat operasional, dan beban kerja Anda memerlukan identitas untuk membuat permintaan ke AWS layanan - misalnya, untuk membaca data. Identitas ini mencakup mesin yang berjalan di AWS lingkunga n Anda seperti EC2 instans Amazon atau fungsi Lambda AWS . Anda juga dapat mengelola identitas mesin untuk pihak eksternal yang membutuhkan akses. Selain itu, Anda mungkin juga memiliki mesin di luar AWS yang membutuhk an akses ke AWS lingkungan Anda.		(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePreve ntion MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 2	Bagaimana Anda mengelola identitas untuk orang dan mesin? Ada dua jenis identitas yang perlu Anda kelola saat mendekati beban AWS kerja yang aman. Memahami jenis identitas yang Anda butuhkan untuk mengelola dan memberikan akses membantu Anda memastikan identitas yang tepat memiliki akses ke sumber daya yang tepat dalam kondisi yang tepat. Identitas Manusia: Administrator, pengembang, operator, dan pengguna akhir Anda memerlukan identitas untuk mengakses AWS lingkungan dan aplikasi Anda. Ini adalah anggota organisasi Anda, atau pengguna eksternal dengan siapa Anda berkolaborasi, dan yang berinteraksi	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dengan AWS sumber daya Anda dari browser web, aplikasi klien, atau alat baris perintah interakti f. Identitas Mesin: Aplikasi layanan, alat operasional, dan beban kerja Anda memerlukan identitas untuk membuat permintaan ke AWS layanan - misalnya, untuk membaca data. Identitas ini mencakup mesin yang berjalan di AWS lingkunga n Anda seperti EC2 instans Amazon atau fungsi Lambda AWS . Anda juga dapat mengelola identitas mesin untuk pihak eksternal yang membutuhkan akses. Selain itu, Anda mungkin juga memiliki mesin di luar AWS yang membutuhk an akses ke AWS lingkungan Anda.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 2	Bagaimana Anda mengelola identitas untuk orang dan mesin? Ada dua jenis identitas yang perlu Anda kelola saat mendekati beban AWS kerja yang aman. Memahami jenis identitas yang Anda butuhkan untuk mengelola dan memberikan akses membantu Anda memastikan identitas yang tepat memiliki akses ke sumber daya yang tepat dalam kondisi yang tepat. Identitas Manusia: Administrator, pengembang, operator, dan pengguna akhir Anda memerlukan identitas untuk mengakses AWS lingkungan dan aplikasi Anda. Ini adalah anggota organisasi Anda, atau pengguna eksternal dengan siapa Anda berkolaborasi, dan yang berinteraksi	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dengan AWS sumber daya Anda dari browser web, aplikasi klien, atau alat baris perintah interakti f. Identitas Mesin: Aplikasi layanan, alat operasional, dan beban kerja Anda memerlukan identitas untuk membuat permintaan ke AWS layanan - misalnya, untuk membaca data. Identitas ini mencakup mesin yang berjalan di AWS lingkunga n Anda seperti EC2 instans Amazon atau fungsi Lambda AWS . Anda juga dapat mengelola identitas mesin untuk pihak eksternal yang membutuhkan akses. Selain itu, Anda mungkin juga memiliki mesin di luar AWS yang membutuhk an akses ke AWS lingkungan Anda.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 2	Bagaimana Anda mengelola identitas untuk orang dan mesin? Ada dua jenis identitas yang perlu Anda kelola saat mendekati beban AWS kerja yang aman. Memahami jenis identitas yang Anda butuhkan untuk mengelola dan memberikan akses membantu Anda memastikan identitas yang tepat memiliki akses ke sumber daya yang tepat dalam kondisi yang tepat. Identitas Manusia: Administrator, pengembang, operator, dan pengguna akhir Anda memerlukan identitas untuk mengakses AWS lingkungan dan aplikasi Anda. Ini adalah anggota organisasi Anda, atau pengguna eksternal dengan siapa Anda berkolaborasi, dan yang berinteraksi	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dengan AWS sumber daya Anda dari browser web, aplikasi klien, atau alat baris perintah interakti f. Identitas Mesin: Aplikasi layanan, alat operasional, dan beban kerja Anda memerlukan identitas untuk membuat permintaan ke AWS layanan - misalnya, untuk membaca data. Identitas ini mencakup mesin yang berjalan di AWS lingkunga n Anda seperti EC2 instans Amazon atau fungsi Lambda AWS . Anda juga dapat mengelola identitas mesin untuk pihak eksternal yang membutuhkan akses. Selain itu, Anda mungkin juga memiliki mesin di luar AWS yang membutuhk an akses ke AWS lingkungan Anda.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 2	Bagaimana Anda mengelola identitas untuk orang dan mesin? Ada dua jenis identitas yang perlu Anda kelola saat mendekati beban AWS kerja yang aman. Memahami jenis identitas yang Anda butuhkan untuk mengelola dan memberikan akses membantu Anda memastikan identitas yang tepat memiliki akses ke sumber daya yang tepat dalam kondisi yang tepat. Identitas Manusia: Administrator, pengembang, operator, dan pengguna akhir Anda memerlukan identitas untuk mengakses AWS lingkungan dan aplikasi Anda. Ini adalah anggota organisasi Anda, atau pengguna eksternal dengan siapa Anda berkolaborasi, dan yang berinteraksi	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dengan AWS sumber daya Anda dari browser web, aplikasi klien, atau alat baris perintah interakti f. Identitas Mesin: Aplikasi layanan, alat operasional, dan beban kerja Anda memerlukan identitas untuk membuat permintaan ke AWS layanan - misalnya, untuk membaca data. Identitas ini mencakup mesin yang berjalan di AWS lingkunga n Anda seperti EC2 instans Amazon atau fungsi Lambda AWS . Anda juga dapat mengelola identitas mesin untuk pihak eksternal yang membutuhkan akses. Selain itu, Anda mungkin juga memiliki mesin di luar AWS yang membutuhk an akses ke AWS lingkungan Anda.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 2	Bagaimana Anda mengelola identitas untuk orang dan mesin? Ada dua jenis identitas yang perlu Anda kelola saat mendekati beban AWS kerja yang aman. Memahami jenis identitas yang Anda butuhkan untuk mengelola dan memberikan akses membantu Anda memastikan identitas yang tepat memiliki akses ke sumber daya yang tepat dalam kondisi yang tepat. Identitas Manusia: Administrator, pengembang, operator, dan pengguna akhir Anda memerlukan identitas untuk mengakses AWS lingkungan dan aplikasi Anda. Ini adalah anggota organisasi Anda, atau pengguna eksternal dengan siapa Anda berkolaborasi, dan yang berinteraksi	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dengan AWS sumber daya Anda dari browser web, aplikasi klien, atau alat baris perintah interakti f. Identitas Mesin: Aplikasi layanan, alat operasional, dan beban kerja Anda memerlukan identitas untuk membuat permintaan ke AWS layanan - misalnya, untuk membaca data. Identitas ini mencakup mesin yang berjalan di AWS lingkunga n Anda seperti EC2 instans Amazon atau fungsi Lambda AWS . Anda juga dapat mengelola identitas mesin untuk pihak eksternal yang membutuhkan akses. Selain itu, Anda mungkin juga memiliki mesin di luar AWS yang membutuhk an akses ke AWS lingkungan Anda.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 2	Bagaimana Anda mengelola identitas untuk orang dan mesin? Ada dua jenis identitas yang perlu Anda kelola saat mendekati beban AWS kerja yang aman. Memahami jenis identitas yang Anda butuhkan untuk mengelola dan memberikan akses membantu Anda memastikan identitas yang tepat memiliki akses ke sumber daya yang tepat dalam kondisi yang tepat. Identitas Manusia: Administrator, pengembang, operator, dan pengguna akhir Anda memerlukan identitas untuk mengakses AWS lingkungan dan aplikasi Anda. Ini adalah anggota organisasi Anda, atau pengguna eksternal dengan siapa Anda berkolaborasi, dan yang berinteraksi	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dengan AWS sumber daya Anda dari browser web, aplikasi klien, atau alat baris perintah interakti f. Identitas Mesin: Aplikasi layanan, alat operasional, dan beban kerja Anda memerlukan identitas untuk membuat permintaan ke AWS layanan - misalnya, untuk membaca data. Identitas ini mencakup mesin yang berjalan di AWS lingkunga n Anda seperti EC2 instans Amazon atau fungsi Lambda AWS . Anda juga dapat mengelola identitas mesin untuk pihak eksternal yang membutuhkan akses. Selain itu, Anda mungkin juga memiliki mesin di luar AWS yang membutuhk an akses ke AWS lingkungan Anda.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 2	Bagaimana Anda mengelola identitas untuk orang dan mesin? Ada dua jenis identitas yang perlu Anda kelola saat mendekati beban AWS kerja yang aman. Memahami jenis identitas yang Anda butuhkan untuk mengelola dan memberikan akses membantu Anda memastikan identitas yang tepat memiliki akses ke sumber daya yang tepat dalam kondisi yang tepat. Identitas Manusia: Administrator, pengembang, operator, dan pengguna akhir Anda memerlukan identitas untuk mengakses AWS lingkungan dan aplikasi Anda. Ini adalah anggota organisasi Anda, atau pengguna eksternal dengan siapa Anda berkolaborasi, dan yang berinteraksi	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dengan AWS sumber daya Anda dari browser web, aplikasi klien, atau alat baris perintah interakti f. Identitas Mesin: Aplikasi layanan, alat operasional, dan beban kerja Anda memerlukan identitas untuk membuat permintaan ke AWS layanan - misalnya, untuk membaca data. Identitas ini mencakup mesin yang berjalan di AWS lingkunga n Anda seperti EC2 instans Amazon atau fungsi Lambda AWS . Anda juga dapat mengelola identitas mesin untuk pihak eksternal yang membutuhkan akses. Selain itu, Anda mungkin juga memiliki mesin di luar AWS yang membutuhk an akses ke AWS lingkungan Anda.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 2	Bagaimana Anda mengelola identitas untuk orang dan mesin? Ada dua jenis identitas yang perlu Anda kelola saat mendekati beban AWS kerja yang aman. Memahami jenis identitas yang Anda butuhkan untuk mengelola dan memberikan akses membantu Anda memastikan identitas yang tepat memiliki akses ke sumber daya yang tepat dalam kondisi yang tepat. Identitas Manusia: Administrator, pengembang, operator, dan pengguna akhir Anda memerlukan identitas untuk mengakses AWS lingkungan dan aplikasi Anda. Ini adalah anggota organisasi Anda, atau pengguna eksternal dengan siapa Anda berkolaborasi, dan yang berinteraksi	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dengan AWS sumber daya Anda dari browser web, aplikasi klien, atau alat baris perintah interakti f. Identitas Mesin: Aplikasi layanan, alat operasional, dan beban kerja Anda memerlukan identitas untuk membuat permintaan ke AWS layanan - misalnya, untuk membaca data. Identitas ini mencakup mesin yang berjalan di AWS lingkunga n Anda seperti EC2 instans Amazon atau fungsi Lambda AWS . Anda juga dapat mengelola identitas mesin untuk pihak eksternal yang membutuhkan akses. Selain itu, Anda mungkin juga memiliki mesin di luar AWS yang membutuhk an akses ke AWS lingkungan Anda.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 2	Bagaimana Anda mengelola identitas untuk orang dan mesin? Ada dua jenis identitas yang perlu Anda kelola saat mendekati beban AWS kerja yang aman. Memahami jenis identitas yang Anda butuhkan untuk mengelola dan memberikan akses membantu Anda memastikan identitas yang tepat memiliki akses ke sumber daya yang tepat dalam kondisi yang tepat. Identitas Manusia: Administrator, pengembang, operator, dan pengguna akhir Anda memerlukan identitas untuk mengakses AWS lingkungan dan aplikasi Anda. Ini adalah anggota organisasi Anda, atau pengguna eksternal dengan siapa Anda berkolaborasi, dan yang berinteraksi	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dengan AWS sumber daya Anda dari browser web, aplikasi klien, atau alat baris perintah interakti f. Identitas Mesin: Aplikasi layanan, alat operasional, dan beban kerja Anda memerlukan identitas untuk membuat permintaan ke AWS layanan - misalnya, untuk membaca data. Identitas ini mencakup mesin yang berjalan di AWS lingkunga n Anda seperti EC2 instans Amazon atau fungsi Lambda AWS . Anda juga dapat mengelola identitas mesin untuk pihak eksternal yang membutuhkan akses. Selain itu, Anda mungkin juga memiliki mesin di luar AWS yang membutuhk an akses ke AWS lingkungan Anda.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 2	Bagaimana Anda mengelola identitas untuk orang dan mesin? Ada dua jenis identitas yang perlu Anda kelola saat mendekati beban AWS kerja yang aman. Memahami jenis identitas yang Anda butuhkan untuk mengelola dan memberikan akses membantu Anda memastikan identitas yang tepat memiliki akses ke sumber daya yang tepat dalam kondisi yang tepat. Identitas Manusia: Administrator, pengembang, operator, dan pengguna akhir Anda memerlukan identitas untuk mengakses AWS lingkungan dan aplikasi Anda. Ini adalah anggota organisasi Anda, atau pengguna eksternal dengan siapa Anda berkolaborasi, dan yang berinteraksi	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dengan AWS sumber daya Anda dari browser web, aplikasi klien, atau alat baris perintah interakti f. Identitas Mesin: Aplikasi layanan, alat operasional, dan beban kerja Anda memerlukan identitas untuk membuat permintaan ke AWS layanan - misalnya, untuk membaca data. Identitas ini mencakup mesin yang berjalan di AWS lingkunga n Anda seperti EC2 instans Amazon atau fungsi Lambda AWS . Anda juga dapat mengelola identitas mesin untuk pihak eksternal yang membutuhkan akses. Selain itu, Anda mungkin juga memiliki mesin di luar AWS yang membutuhk an akses ke AWS lingkungan Anda.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 2	Bagaimana Anda mengelola identitas untuk orang dan mesin? Ada dua jenis identitas yang perlu Anda kelola saat mendekati beban AWS kerja yang aman. Memahami jenis identitas yang Anda butuhkan untuk mengelola dan memberikan akses membantu Anda memastikan identitas yang tepat memiliki akses ke sumber daya yang tepat dalam kondisi yang tepat. Identitas Manusia: Administrator, pengembang, operator, dan pengguna akhir Anda memerlukan identitas untuk mengakses AWS lingkungan dan aplikasi Anda. Ini adalah anggota organisasi Anda, atau pengguna eksternal dengan siapa Anda berkolaborasi, dan yang berinteraksi	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dengan AWS sumber daya Anda dari browser web, aplikasi klien, atau alat baris perintah interakti f. Identitas Mesin: Aplikasi layanan, alat operasional, dan beban kerja Anda memerlukan identitas untuk membuat permintaan ke AWS layanan - misalnya, untuk membaca data. Identitas ini mencakup mesin yang berjalan di AWS lingkunga n Anda seperti EC2 instans Amazon atau fungsi Lambda AWS . Anda juga dapat mengelola identitas mesin untuk pihak eksternal yang membutuhkan akses. Selain itu, Anda mungkin juga memiliki mesin di luar AWS yang membutuhk an akses ke AWS lingkungan Anda.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 2	Bagaimana Anda mengelola identitas untuk orang dan mesin? Ada dua jenis identitas yang perlu Anda kelola saat mendekati beban AWS kerja yang aman. Memahami jenis identitas yang Anda butuhkan untuk mengelola dan memberikan akses membantu Anda memastikan identitas yang tepat memiliki akses ke sumber daya yang tepat dalam kondisi yang tepat. Identitas Manusia: Administrator, pengembang, operator, dan pengguna akhir Anda memerlukan identitas untuk mengakses AWS lingkungan dan aplikasi Anda. Ini adalah anggota organisasi Anda, atau pengguna eksternal dengan siapa Anda berkolaborasi, dan yang berinteraksi	secretsmanager-rotation-enabled-check	Aturan ini memastikan AWS rahasia Secrets Manager telah diaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dengan AWS sumber daya Anda dari browser web, aplikasi klien, atau alat baris perintah interakti f. Identitas Mesin: Aplikasi layanan, alat operasional, dan beban kerja Anda memerlukan identitas untuk membuat permintaan ke AWS layanan - misalnya, untuk membaca data. Identitas ini mencakup mesin yang berjalan di AWS lingkunga n Anda seperti EC2 instans Amazon atau fungsi Lambda AWS . Anda juga dapat mengelola identitas mesin untuk pihak eksternal yang membutuhkan akses. Selain itu, Anda mungkin juga memiliki mesin di luar AWS yang membutuhk an akses ke AWS lingkungan Anda.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 2	Bagaimana Anda mengelola identitas untuk orang dan mesin? Ada dua jenis identitas yang perlu Anda kelola saat mendekati beban AWS kerja yang aman. Memahami jenis identitas yang Anda butuhkan untuk mengelola dan memberikan akses membantu Anda memastikan identitas yang tepat memiliki akses ke sumber daya yang tepat dalam kondisi yang tepat. Identitas Manusia: Administrator, pengembang, operator, dan pengguna akhir Anda memerlukan identitas untuk mengakses AWS lingkungan dan aplikasi Anda. Ini adalah anggota organisasi Anda, atau pengguna eksternal dengan siapa Anda berkolaborasi, dan yang berinteraksi	secretsmanager-scheduled-rotation-success-periksa	Aturan ini memastikan bahwa AWS rahasia Secrets Manager telah berhasil diputar sesuai dengan jadwal rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode di mana rahasia aktif, dan berpotensi mengurangi dampak bisnis jika dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dengan AWS sumber daya Anda dari browser web, aplikasi klien, atau alat baris perintah interakti f. Identitas Mesin: Aplikasi layanan, alat operasional, dan beban kerja Anda memerlukan identitas untuk membuat permintaan ke AWS layanan - misalnya, untuk membaca data. Identitas ini mencakup mesin yang berjalan di AWS lingkunga n Anda seperti EC2 instans Amazon atau fungsi Lambda AWS . Anda juga dapat mengelola identitas mesin untuk pihak eksternal yang membutuhkan akses. Selain itu, Anda mungkin juga memiliki mesin di luar AWS yang membutuhk an akses ke AWS lingkungan Anda.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 2	Bagaimana Anda mengelola identitas untuk orang dan mesin? Ada dua jenis identitas yang perlu Anda kelola saat mendekati beban AWS kerja yang aman. Memahami jenis identitas yang Anda butuhkan untuk mengelola dan memberikan akses membantu Anda memastikan identitas yang tepat memiliki akses ke sumber daya yang tepat dalam kondisi yang tepat. Identitas Manusia: Administrator, pengembang, operator, dan pengguna akhir Anda memerlukan identitas untuk mengakses AWS lingkungan dan aplikasi Anda. Ini adalah anggota organisasi Anda, atau pengguna eksternal dengan siapa Anda berkolaborasi, dan yang berinteraksi	secretsmanager-secret-periodic-rotation	Aturan ini memastikan AWS rahasia Secrets Manager mengaktifkan rotasi periodik. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan. Nilai defaultnya adalah 90 hari.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dengan AWS sumber daya Anda dari browser web, aplikasi klien, atau alat baris perintah interakti f. Identitas Mesin: Aplikasi layanan, alat operasional, dan beban kerja Anda memerlukan identitas untuk membuat permintaan ke AWS layanan - misalnya, untuk membaca data. Identitas ini mencakup mesin yang berjalan di AWS lingkunga n Anda seperti EC2 instans Amazon atau fungsi Lambda AWS . Anda juga dapat mengelola identitas mesin untuk pihak eksternal yang membutuhkan akses. Selain itu, Anda mungkin juga memiliki mesin di luar AWS yang membutuhk an akses ke AWS lingkungan Anda.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 2	Bagaimana Anda mengelola identitas untuk orang dan mesin? Ada dua jenis identitas yang perlu Anda kelola saat mendekati beban AWS kerja yang aman. Memahami jenis identitas yang Anda butuhkan untuk mengelola dan memberikan akses membantu Anda memastikan identitas yang tepat memiliki akses ke sumber daya yang tepat dalam kondisi yang tepat. Identitas Manusia: Administrator, pengembang, operator, dan pengguna akhir Anda memerlukan identitas untuk mengakses AWS lingkungan dan aplikasi Anda. Ini adalah anggota organisasi Anda, atau pengguna eksternal dengan siapa Anda berkolaborasi, dan yang berinteraksi	secretsmanager-secret-unused	Jika kredensyal yang tidak digunakan ada di AWS Secrets Manager, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa terkecil. Aturan ini memungkinkan Anda untuk menetapkan nilai ke unusedForDays (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dengan AWS sumber daya Anda dari browser web, aplikasi klien, atau alat baris perintah interakti f. Identitas Mesin: Aplikasi layanan, alat operasional, dan beban kerja Anda memerlukan identitas untuk membuat permintaan ke AWS layanan - misalnya, untuk membaca data. Identitas ini mencakup mesin yang berjalan di AWS lingkunga n Anda seperti EC2 instans Amazon atau fungsi Lambda AWS . Anda juga dapat mengelola identitas mesin untuk pihak eksternal yang membutuhkan akses. Selain itu, Anda mungkin juga memiliki mesin di luar AWS yang membutuhk an akses ke AWS lingkungan Anda.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 2	Bagaimana Anda mengelola identitas untuk orang dan mesin? Ada dua jenis identitas yang perlu Anda kelola saat mendekati beban AWS kerja yang aman. Memahami jenis identitas yang Anda butuhkan untuk mengelola dan memberikan akses membantu Anda memastikan identitas yang tepat memiliki akses ke sumber daya yang tepat dalam kondisi yang tepat. Identitas Manusia: Administrator, pengembang, operator, dan pengguna akhir Anda memerlukan identitas untuk mengakses AWS lingkungan dan aplikasi Anda. Ini adalah anggota organisasi Anda, atau pengguna eksternal dengan siapa Anda berkolaborasi, dan yang berinteraksi	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dengan AWS sumber daya Anda dari browser web, aplikasi klien, atau alat baris perintah interakti f. Identitas Mesin: Aplikasi layanan, alat operasional, dan beban kerja Anda memerlukan identitas untuk membuat permintaan ke AWS layanan - misalnya, untuk membaca data. Identitas ini mencakup mesin yang berjalan di AWS lingkunga n Anda seperti EC2 instans Amazon atau fungsi Lambda AWS . Anda juga dapat mengelola identitas mesin untuk pihak eksternal yang membutuhkan akses. Selain itu, Anda mungkin juga memiliki mesin di luar AWS yang membutuhk an akses ke AWS lingkungan Anda.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 2	Bagaimana Anda mengelola identitas untuk orang dan mesin? Ada dua jenis identitas yang perlu Anda kelola saat mendekati beban AWS kerja yang aman. Memahami jenis identitas yang Anda butuhkan untuk mengelola dan memberikan akses membantu Anda memastikan identitas yang tepat memiliki akses ke sumber daya yang tepat dalam kondisi yang tepat. Identitas Manusia: Administrator, pengembang, operator, dan pengguna akhir Anda memerlukan identitas untuk mengakses AWS lingkungan dan aplikasi Anda. Ini adalah anggota organisasi Anda, atau pengguna eksternal dengan siapa Anda berkolaborasi, dan yang berinteraksi	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dengan AWS sumber daya Anda dari browser web, aplikasi klien, atau alat baris perintah interakti f. Identitas Mesin: Aplikasi layanan, alat operasional, dan beban kerja Anda memerlukan identitas untuk membuat permintaan ke AWS layanan - misalnya, untuk membaca data. Identitas ini mencakup mesin yang berjalan di AWS lingkunga n Anda seperti EC2 instans Amazon atau fungsi Lambda AWS . Anda juga dapat mengelola identitas mesin untuk pihak eksternal yang membutuhkan akses. Selain itu, Anda mungkin juga memiliki mesin di luar AWS yang membutuhk an akses ke AWS lingkungan Anda.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Tiap-tiap komponen atau sumber daya beban kerja Anda perlu diakses oleh administrator, pengguna akhir, atau komponen-komponen lainnya. Penetapan harus jelas tentang siapa atau apa yang harus memiliki akses ke tiap-tiap komponen, pilih tipe identitas dan metode autentikasi serta otorisasi yang sesuai.	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Tiap-tiap komponen atau sumber daya beban kerja Anda perlu diakses oleh administrator, pengguna akhir, atau komponen-komponen lainnya. Penetapan harus jelas tentang siapa atau apa yang harus memiliki akses ke tiap-tiap komponen, pilih tipe identitas dan metode autentikasi serta otorisasi yang sesuai.	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Tiap-tiap komponen atau sumber daya beban kerja Anda perlu diakses oleh administrator, pengguna akhir, atau komponen-komponen lainnya. Penetapan harus jelas tentang siapa atau apa yang harus memiliki akses ke tiap-tiap komponen, pilih tipe identitas dan metode autentikasi serta otorisasi yang sesuai.	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Tiap-tiap komponen atau sumber daya beban kerja Anda perlu diakses oleh administrator, pengguna akhir, atau komponen-komponen lainnya. Penetapan harus jelas tentang siapa atau apa yang harus memiliki akses ke tiap-tiap komponen, pilih tipe identitas dan metode autentikasi serta otorisasi yang sesuai.	ecs-task-definition-nonroot-pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan bahwa pengguna non-root ditunjuk untuk mengakses definisi tugas Amazon Elastic Container Service (Amazon ECS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Tiap-tiap komponen atau sumber daya beban kerja Anda perlu diakses oleh administrator, pengguna akhir, atau komponen-komponen lainnya. Penetapan harus jelas tentang siapa atau apa yang harus memiliki akses ke tiap-tiap komponen, pilih tipe identitas dan metode autentikasi serta otorisasi yang sesuai.	ecs-containers-non privileged	Untuk membantu menerapkan prinsip hak istimewa paling rendah, definisi tugas Amazon Elastic Container Service (Amazon ECS) seharusnya tidak mengaktifkan hak istimewa yang ditinggikan. Ketika parameter ini benar, wadah diberikan hak istimewa yang ditinggikan pada instance wadah host (mirip dengan pengguna root).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Tiap-tiap komponen atau sumber daya beban kerja Anda perlu diakses oleh administrator, pengguna akhir, atau komponen-komponen lainnya. Penetapan harus jelas tentang siapa atau apa yang harus memiliki akses ke tiap-tiap komponen, pilih tipe identitas dan metode autentikasi serta otorisasi yang sesuai.	ecs-containers-readonly-access	Mengaktifkan akses baca saja ke wadah Amazon Elastic Container Service (ECS) dapat membantu mematuhi prinsip hak istimewa yang paling rendah. Opsi ini dapat mengurangi vektor serangan karena sistem file instance container tidak dapat dimodifikasi kecuali jika memiliki izin baca-tulis eksplisit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Tiap-tiap komponen atau sumber daya beban kerja Anda perlu diakses oleh administrator, pengguna akhir, atau komponen-komponen lainnya. Penetapan harus jelas tentang siapa atau apa yang harus memiliki akses ke tiap-tiap komponen, pilih tipe identitas dan metode autentikasi serta otorisasi yang sesuai.	efs-access-point-enforce-identitas pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan penegakan pengguna diaktifkan untuk Amazon Elastic File System (Amazon EFS) Anda. Saat diaktifkan, Amazon EFS mengganti kan pengguna dan grup klien NFS IDs dengan identitas yang dikonfigurasi pada titik akses untuk semua operasi sistem file dan hanya memberika n akses ke identitas pengguna yang diberlakukan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Tiap-tiap komponen atau sumber daya beban kerja Anda perlu diakses oleh administrator, pengguna akhir, atau komponen-komponen lainnya. Penetapan harus jelas tentang siapa atau apa yang harus memiliki akses ke tiap-tiap komponen, pilih tipe identitas dan metode autentikasi serta otorisasi yang sesuai.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktifkan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediakan sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Tiap-tiap komponen atau sumber daya beban kerja Anda perlu diakses oleh administrator, pengguna akhir, atau komponen-komponen lainnya. Penetapan harus jelas tentang siapa atau apa yang harus memiliki akses ke tiap-tiap komponen, pilih tipe identitas dan metode autentikasi serta otorisasi yang sesuai.	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Tiap-tiap komponen atau sumber daya beban kerja Anda perlu diakses oleh administrator, pengguna akhir, atau komponen-komponen lainnya. Penetapan harus jelas tentang siapa atau apa yang harus memiliki akses ke tiap-tiap komponen, pilih tipe identitas dan metode autentikasi serta otorisasi yang sesuai.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Tiap-tiap komponen atau sumber daya beban kerja Anda perlu diakses oleh administrator, pengguna akhir, atau komponen-komponen lainnya. Penetapan harus jelas tentang siapa atau apa yang harus memiliki akses ke tiap-tiap komponen, pilih tipe identitas dan metode autentikasi serta otorisasi yang sesuai.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Tiap-tiap komponen atau sumber daya beban kerja Anda perlu diakses oleh administrator, pengguna akhir, atau komponen-komponen lainnya. Penetapan harus jelas tentang siapa atau apa yang harus memiliki akses ke tiap-tiap komponen, pilih tipe identitas dan metode autentikasi serta otorisasi yang sesuai.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Tiap-tiap komponen atau sumber daya beban kerja Anda perlu diakses oleh administrator, pengguna akhir, atau komponen-komponen lainnya. Penetapan harus jelas tentang siapa atau apa yang harus memiliki akses ke tiap-tiap komponen, pilih tipe identitas dan metode autentikasi serta otorisasi yang sesuai.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Tiap-tiap komponen atau sumber daya beban kerja Anda perlu diakses oleh administrator, pengguna akhir, atau komponen-komponen lainnya. Penetapan harus jelas tentang siapa atau apa yang harus memiliki akses ke tiap-tiap komponen, pilih tipe identitas dan metode autentikasi serta otorisasi yang sesuai.	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Tiap-tiap komponen atau sumber daya beban kerja Anda perlu diakses oleh administrator, pengguna akhir, atau komponen-komponen lainnya. Penetapan harus jelas tentang siapa atau apa yang harus memiliki akses ke tiap-tiap komponen, pilih tipe identitas dan metode autentikasi serta otorisasi yang sesuai.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Tiap-tiap komponen atau sumber daya beban kerja Anda perlu diakses oleh administrator, pengguna akhir, atau komponen-komponen lainnya. Penetapan harus jelas tentang siapa atau apa yang harus memiliki akses ke tiap-tiap komponen, pilih tipe identitas dan metode autentikasi serta otorisasi yang sesuai.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Tiap-tiap komponen atau sumber daya beban kerja Anda perlu diakses oleh administrator, pengguna akhir, atau komponen-komponen lainnya. Penetapan harus jelas tentang siapa atau apa yang harus memiliki akses ke tiap-tiap komponen, pilih tipe identitas dan metode autentikasi serta otorisasi yang sesuai.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Tiap-tiap komponen atau sumber daya beban kerja Anda perlu diakses oleh administrator, pengguna akhir, atau komponen-komponen lainnya. Penetapan harus jelas tentang siapa atau apa yang harus memiliki akses ke tiap-tiap komponen, pilih tipe identitas dan metode autentikasi serta otorisasi yang sesuai.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Tetapkan kontrol umum yang membatasi akses ke semua identitas di organisasi Anda. Misalnya, Anda dapat membatasi akses ke AWS Wilayah tertentu, atau mencegah operator menghapus sumber daya umum, seperti peran IAM yang digunakan untuk tim keamanan pusat Anda	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Terus memantau temuan yang menyoroti akses publik dan lintas akun. Kurangi akses publik dan akses lintas akun hanya ke sumber daya yang memerlukan jenis akses ini.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Terus memantau temuan yang menyoroti akses publik dan lintas akun. Kurangi akses publik dan akses lintas akun hanya ke sumber daya yang memerluka n jenis akses ini.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Terus memantau temuan yang menyoroti akses publik dan lintas akun. Kurangi akses publik dan akses lintas akun hanya ke sumber daya yang memerluka n jenis akses ini.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Terus memantau temuan yang menyoroti akses publik dan lintas akun. Kurangi akses publik dan akses lintas akun hanya ke sumber daya yang memerlukan jenis akses ini.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Terus memantau temuan yang menyoroti akses publik dan lintas akun. Kurangi akses publik dan akses lintas akun hanya ke sumber daya yang memerlukan jenis akses ini.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Terus memantau temuan yang menyoroti akses publik dan lintas akun. Kurangi akses publik dan akses lintas akun hanya ke sumber daya yang memerlukan jenis akses ini.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Terus memantau temuan yang menyoroti akses publik dan lintas akun. Kurangi akses publik dan akses lintas akun hanya ke sumber daya yang memerluka n jenis akses ini.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Terus memantau temuan yang menyoroti akses publik dan lintas akun. Kurangi akses publik dan akses lintas akun hanya ke sumber daya yang memerlukan jenis akses ini.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Terus memantau temuan yang menyoroti akses publik dan lintas akun. Kurangi akses publik dan akses lintas akun hanya ke sumber daya yang memerluka n jenis akses ini.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Terus memantau temuan yang menyoroti akses publik dan lintas akun. Kurangi akses publik dan akses lintas akun hanya ke sumber daya yang memerluka n jenis akses ini.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Terus memantau temuan yang menyoroti akses publik dan lintas akun. Kurangi akses publik dan akses lintas akun hanya ke sumber daya yang memerluka n jenis akses ini.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Terus memantau temuan yang menyoroti akses publik dan lintas akun. Kurangi akses publik dan akses lintas akun hanya ke sumber daya yang memerlukan jenis akses ini.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Terus memantau temuan yang menyoroti akses publik dan lintas akun. Kurangi akses publik dan akses lintas akun hanya ke sumber daya yang memerlukan jenis akses ini.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Terus memantau temuan yang menyoroti akses publik dan lintas akun. Kurangi akses publik dan akses lintas akun hanya ke sumber daya yang memerlukan jenis akses ini.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Terus memantau temuan yang menyoroti akses publik dan lintas akun. Kurangi akses publik dan akses lintas akun hanya ke sumber daya yang memerlukan jenis akses ini.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Terus memantau temuan yang menyoroti akses publik dan lintas akun. Kurangi akses publik dan akses lintas akun hanya ke sumber daya yang memerlukan jenis akses ini.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Terus memantau temuan yang menyoroti akses publik dan lintas akun. Kurangi akses publik dan akses lintas akun hanya ke sumber daya yang memerlukan jenis akses ini.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Terus memantau temuan yang menyoroti akses publik dan lintas akun. Kurangi akses publik dan akses lintas akun hanya ke sumber daya yang memerlukan jenis akses ini.	secretsmanager-secret-unused	Jika kredensyal yang tidak digunakan ada di AWS Secrets Manager, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa terkecil. Aturan ini memungkinkan Anda untuk menetapkan nilai ke unusedForDays (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Terus memantau temuan yang menyoroti akses publik dan lintas akun. Kurangi akses publik dan akses lintas akun hanya ke sumber daya yang memerlukan jenis akses ini.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Terus memantau temuan yang menyoroti akses publik dan lintas akun. Kurangi akses publik dan akses lintas akun hanya ke sumber daya yang memerlukan jenis akses ini.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
DTK 3	Bagaimana cara mengelola izin untuk manusia dan mesin? Terus memantau temuan yang menyoroti akses publik dan lintas akun. Kurangi akses publik dan akses lintas akun hanya ke sumber daya yang memerlukan jenis akses ini.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 4	Bagaimana cara mendeteksi dan menyelidiki peristiwa keamanan? Catat dan analisis peristiwa dari log dan metrik untuk mendapatkan visibilitas. Ambil tindakan atas peristiwa keamanan dan potensi ancaman untuk membantu mengamankan beban kerja Anda.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
DTK 4	Bagaimana cara mendeteksi dan menyelidiki peristiwa keamanan? Catat dan analisis peristiwa dari log dan metrik untuk mendapatkan visibilitas. Ambil tindakan atas peristiwa keamanan dan potensi ancaman untuk membantu mengamankan beban kerja Anda.	opensearch-audit-logging-enabled	Pastikan pencatatan audit diaktifkan di domain OpenSearch Layanan Amazon Anda. Pencatatan audit memungkinkan Anda melacak aktivitas pengguna di OpenSearch domain Anda, termasuk keberhasilan dan kegagalan otentikasi, permintaan, perubahan indeks OpenSearch, dan kueri penelusuran yang masuk.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 4	Bagaimana cara mendeteksi dan menyelidiki peristiwa keamanan? Catat dan analisis peristiwa dari log dan metrik untuk mendapatk an visibilitas. Ambil tindakan atas peristiwa keamanan dan potensi ancaman untuk membantu mengamankan beban kerja Anda.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
DTK 4	Bagaimana cara mendeteksi dan menyelidiki peristiwa keamanan? Catat dan analisis peristiwa dari log dan metrik untuk mendapatk an visibilitas. Ambil tindakan atas peristiwa keamanan dan potensi ancaman untuk membantu mengamankan beban kerja Anda.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteks i aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses objek di bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 4	Bagaimana cara mendeteksi dan menyelidiki peristiwa keamanan? Catat dan analisis peristiwa dari log dan metrik untuk mendapatkan visibilitas. Ambil tindakan atas peristiwa keamanan dan potensi ancaman untuk membantu mengamankan beban kerja Anda.	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.
DTK 4	Bagaimana cara mendeteksi dan menyelidiki peristiwa keamanan? Catat dan analisis peristiwa dari log dan metrik untuk mendapatkan visibilitas. Ambil tindakan atas peristiwa keamanan dan potensi ancaman untuk membantu mengamankan beban kerja Anda.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 4	Bagaimana cara mendeteksi dan menyelidiki peristiwa keamanan? Catat dan analisis peristiwa dari log dan metrik untuk mendapatk an visibilitas. Ambil tindakan atas peristiwa keamanan dan potensi ancaman untuk membantu mengamankan beban kerja Anda.	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 4	Bagaimana cara mendeteksi dan menyelidiki peristiwa keamanan? Catat dan analisis peristiwa dari log dan metrik untuk mendapatk an visibilitas. Ambil tindakan atas peristiwa keamanan dan potensi ancaman untuk membantu mengamankan beban kerja Anda.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 4	Bagaimana cara mendeteksi dan menyelidiki peristiwa keamanan? Catat dan analisis peristiwa dari log dan metrik untuk mendapatk an visibilitas. Ambil tindakan atas peristiwa keamanan dan potensi ancaman untuk membantu mengamankan beban kerja Anda.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 4	Bagaimana cara mendeteksi dan menyelidiki peristiwa keamanan? Catat dan analisis peristiwa dari log dan metrik untuk mendapatk an visibilitas. Ambil tindakan atas peristiwa keamanan dan potensi ancaman untuk membantu mengamankan beban kerja Anda.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 4	Bagaimana cara mendeteksi dan menyelidiki peristiwa keamanan? Catat dan analisis peristiwa dari log dan metrik untuk mendapatkan visibilitas. Ambil tindakan atas peristiwa keamanan dan potensi ancaman untuk membantu mengamankan beban kerja Anda.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 4	Bagaimana cara mendeteksi dan menyelidiki peristiwa keamanan? Catat dan analisis peristiwa dari log dan metrik untuk mendapatk an visibilitas. Ambil tindakan atas peristiwa keamanan dan potensi ancaman untuk membantu mengamankan beban kerja Anda.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 4	Bagaimana cara mendeteksi dan menyelidiki peristiwa keamanan? Catat dan analisis peristiwa dari log dan metrik untuk mendapatkan visibilitas. Ambil tindakan atas peristiwa keamanan dan potensi ancaman untuk membantu mengamankan beban kerja Anda.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 4	Bagaimana cara mendeteksi dan menyelidiki peristiwa keamanan? Catat dan analisis peristiwa dari log dan metrik untuk mendapatk an visibilitas. Ambil tindakan atas peristiwa keamanan dan potensi ancaman untuk membantu mengamankan beban kerja Anda.	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomen dasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaa n enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 4	Bagaimana cara mendeteksi dan menyelidiki peristiwa keamanan? Catat dan analisis peristiwa dari log dan metrik untuk mendapatkan visibilitas. Ambil tindakan atas peristiwa keamanan dan potensi ancaman untuk membantu mengamankan beban kerja Anda.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 4	Bagaimana cara mendeteksi dan menyelidiki peristiwa keamanan? Catat dan analisis peristiwa dari log dan metrik untuk mendapatk an visibilitas. Ambil tindakan atas peristiwa keamanan dan potensi ancaman untuk membantu mengamankan beban kerja Anda.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 4	Bagaimana cara mendeteksi dan menyelidiki peristiwa keamanan? Catat dan analisis peristiwa dari log dan metrik untuk mendapatk an visibilitas. Ambil tindakan atas peristiwa keamanan dan potensi ancaman untuk membantu mengamankan beban kerja Anda.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 4	Bagaimana cara mendeteksi dan menyelidiki peristiwa keamanan? Catat dan analisis peristiwa dari log dan metrik untuk mendapatk an visibilitas. Ambil tindakan atas peristiwa keamanan dan potensi ancaman untuk membantu mengamankan beban kerja Anda.	cloudwatch-alarm-a ction-check	Amazon CloudWatc h mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasark an pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActi onRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman berbasis jaringan eksternal dan internal.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman berbasis jaringan eksternal dan internal.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman berbasis jaringan eksternal dan internal.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman berbasis jaringan eksternal dan internal.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigurasi ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman berbasis jaringan eksternal dan internal.	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositori data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman berbasis jaringan eksternal dan internal.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman berbasis jaringan eksternal dan internal.	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindungiinya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerluka n beberapa lapisan pertahanan untuk membantu melindung i dari ancaman berbasis jaringan eksternal dan internal.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerluka n beberapa lapisan pertahanan untuk membantu melindung i dari ancaman berbasis jaringan eksternal dan internal.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman berbasis jaringan eksternal dan internal.	ec2- instance-multiple-eni-check	Aturan ini memeriksa apakah instans Amazon Elastic Compute Cloud (Amazon EC2) Anda memiliki beberapa. ENIs Memiliki beberapa ENIs dapat menyebabkan instance dual-homed, yang berarti instance yang memiliki beberapa subnet. Ini dapat menambah kompleksitas keamanan jaringan dan memperkenalkan jalur dan akses jaringan yang tidak diinginkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman berbasis jaringan eksternal dan internal.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman berbasis jaringan eksternal dan internal.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman berbasis jaringan eksternal dan internal.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman berbasis jaringan eksternal dan internal.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerluka n beberapa lapisan pertahanan untuk membantu melindung i dari ancaman berbasis jaringan eksternal dan internal.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerluka n beberapa lapisan pertahanan untuk membantu melindung i dari ancaman berbasis jaringan eksternal dan internal.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman berbasis jaringan eksternal dan internal.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman berbasis jaringan eksternal dan internal.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman berbasis jaringan eksternal dan internal.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman berbasis jaringan eksternal dan internal.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman berbasis jaringan eksternal dan internal.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman berbasis jaringan eksternal dan internal.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman berbasis jaringan eksternal dan internal.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman berbasis jaringan eksternal dan internal.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman berbasis jaringan eksternal dan internal.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman berbasis jaringan eksternal dan internal.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman berbasis jaringan eksternal dan internal.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman berbasis jaringan eksternal dan internal.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman berbasis jaringan eksternal dan internal.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 5	Bagaimana cara melindungi sumber daya komputasi Anda? Sumber daya komputasi di beban kerja Anda memerlukan beberapa lapisan pertahanan untuk membantu melindung i dari ancaman eksternal dan internal. Sumber daya komputasi mencakup EC2 instance, kontainer, fungsi AWS Lambda, layanan basis data, perangkat IoT, dan banyak lagi.	waf-regional-rule-not-kosong	Pastikan AWS WAF Anda memiliki aturan yang tidak kosong. Aturan tanpa kondisi dapat mengakibatkan perilaku yang tidak diinginkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 5	Bagaimana cara melindungi sumber daya komputasi Anda? Sumber daya komputasi di beban kerja Anda memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman eksternal dan internal. Sumber daya komputasi mencakup EC2 instance, kontainer, fungsi AWS Lambda, layanan basis data, perangkat IoT, dan banyak lagi.	waf-regional-rulegroup-not-kosong	Pastikan AWS WAF Anda memiliki grup aturan yang tidak kosong. Grup aturan yang kosong dapat mengakibatkan perilaku yang tidak diinginkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 5	Bagaimana cara melindungi sumber daya komputasi Anda? Sumber daya komputasi di beban kerja Anda memerlukan beberapa lapisan pertahanan untuk membantu melindung i dari ancaman eksternal dan internal. Sumber daya komputasi mencakup EC2 instance, kontainer, fungsi AWS Lambda, layanan basis data, perangkat IoT, dan banyak lagi.	waf-regional-webacl-not-kosong	Web ACL yang dilampirkan ke AWS WAF dapat berisi kumpulan aturan dan kelompok aturan untuk memeriksa dan mengontrol permintaan web. Jika ACL Web kosong, lalu lintas web lewat tanpa terdeteksi atau ditindaklanjuti oleh WAF.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 5	Bagaimana cara melindungi sumber daya komputasi Anda? Sumber daya komputasi di beban kerja Anda memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman eksternal dan internal. Sumber daya komputasi mencakup EC2 instance, kontainer, fungsi AWS Lambda, layanan basis data, perangkat IoT, dan banyak lagi.	vpc-network-acl-unused-periksa	Aturan ini memastikan bahwa daftar kontrol akses jaringan Amazon Virtual Private Cloud (VPC) sedang digunakan. Pemantauan untuk daftar kontrol akses jaringan yang tidak digunakan dapat membantu inventaris dan pengelolaan lingkungan Anda yang akurat.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman berbasis jaringan eksternal dan internal.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 5	Bagaimana cara melindungi sumber daya jaringan Anda? Setiap beban kerja yang memiliki beberapa bentuk konektivitas jaringan, apakah itu internet atau jaringan pribadi, memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman berbasis jaringan eksternal dan internal.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 6	Bagaimana cara melindungi sumber daya komputasi Anda? Sumber daya komputasi di beban kerja Anda memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman eksternal dan internal. Sumber daya komputasi mencakup EC2 instance, kontainer, fungsi AWS Lambda, layanan basis data, perangkat IoT, dan banyak lagi.	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relational Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 6	Bagaimana cara melindungi sumber daya komputasi Anda? Sumber daya komputasi di beban kerja Anda memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman eksternal dan internal. Sumber daya komputasi mencakup EC2 instance, kontainer, fungsi AWS Lambda, layanan basis data, perangkat IoT, dan banyak lagi.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 6	Bagaimana cara melindungi sumber daya komputasi Anda? Sumber daya komputasi di beban kerja Anda memerlukan beberapa lapisan pertahanan untuk membantu melindung i dari ancaman eksternal dan internal. Sumber daya komputasi mencakup EC2 instance, kontainer, fungsi AWS Lambda, layanan basis data, perangkat IoT, dan banyak lagi.	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomen dasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaa n enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 6	Bagaimana cara melindungi sumber daya komputasi Anda? Sumber daya komputasi di beban kerja Anda memerlukan beberapa lapisan pertahanan untuk membantu melindung i dari ancaman eksternal dan internal. Sumber daya komputasi mencakup EC2 instance, kontainer, fungsi AWS Lambda, layanan basis data, perangkat IoT, dan banyak lagi.	elastic-beanstalk-managed-updates-di aktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 6	Bagaimana cara melindungi sumber daya komputasi Anda? Sumber daya komputasi di beban kerja Anda memerlukan beberapa lapisan pertahanan untuk membantu melindung i dari ancaman eksternal dan internal. Sumber daya komputasi mencakup EC2 instance, kontainer, fungsi AWS Lambda, layanan basis data, perangkat IoT, dan banyak lagi.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 6	Bagaimana cara melindungi sumber daya komputasi Anda? Sumber daya komputasi di beban kerja Anda memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman eksternal dan internal. Sumber daya komputasi mencakup EC2 instance, kontainer, fungsi AWS Lambda, layanan basis data, perangkat IoT, dan banyak lagi.	ecr-private-image-scanning-diaktifkan	Pemindaian gambar Amazon Elastic Container Repository (ECR) membantu mengidentifikasi kerentanan perangkat lunak dalam gambar kontainer Anda. Mengaktifkan pemindaian gambar pada repositori ECR menambahkan lapisan verifikasi untuk integritas dan keamanan gambar yang disimpan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 6	Bagaimana cara melindungi sumber daya komputasi Anda? Sumber daya komputasi di beban kerja Anda memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman eksternal dan internal. Sumber daya komputasi mencakup EC2 instance, kontainer, fungsi AWS Lambda, layanan basis data, perangkat IoT, dan banyak lagi.	ecs-container-insights-enabled	Pemantauan merupakan bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja Amazon Elastic Container Service (ECS) dan AWS solusi Anda. Wawasan Kontainer juga akan menyediakan informasi diagnostik, seperti kegagalan mengulang kembali kontainer, untuk membantu Anda melakukan isolasi atas masalah dan mengatasi masalah itu dengan cepat.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 6	Bagaimana cara melindungi sumber daya komputasi Anda? Sumber daya komputasi di beban kerja Anda memerlukan beberapa lapisan pertahanan untuk membantu melindung i dari ancaman eksternal dan internal. Sumber daya komputasi mencakup EC2 instance, kontainer, fungsi AWS Lambda, layanan basis data, perangkat IoT, dan banyak lagi.	ecs-fargate-latest-platform-versi	Pembaruan dan tambalan keamanan diterapkan secara otomatis untuk tugas Fargate AWS Anda. Jika ditemukan masalah keamanan yang memengaru hi versi platform AWS Fargate, AWS tambal versi platform. Untuk membantu pengelolaan tambalan tugas Amazon Elastic Container Service (ECS) yang menjalank an AWS Fargate, perbarui tugas mandiri layanan Anda untuk menggunakan versi platform terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 6	Bagaimana cara melindungi sumber daya komputasi Anda? Sumber daya komputasi di beban kerja Anda memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman eksternal dan internal. Sumber daya komputasi mencakup EC2 instance, kontainer, fungsi AWS Lambda, layanan basis data, perangkat IoT, dan banyak lagi.	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 6	Bagaimana cara melindungi sumber daya komputasi Anda? Sumber daya komputasi di beban kerja Anda memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman eksternal dan internal. Sumber daya komputasi mencakup EC2 instance, kontainer, fungsi AWS Lambda, layanan basis data, perangkat IoT, dan banyak lagi.	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 6	Bagaimana cara melindungi sumber daya komputasi Anda? Sumber daya komputasi di beban kerja Anda memerlukan beberapa lapisan pertahanan untuk membantu melindung i dari ancaman eksternal dan internal. Sumber daya komputasi mencakup EC2 instance, kontainer, fungsi AWS Lambda, layanan basis data, perangkat IoT, dan banyak lagi.	ec2- instance-multiple-eni-check	Aturan ini memeriksa apakah instans Amazon Elastic Compute Cloud (Amazon EC2) Anda memiliki beberapa. ENIs Memiliki beberapa ENIs dapat menyebabkan instance dual-homed, yang berarti instance yang memiliki beberapa subnet. Ini dapat menambah kompleksitas keamanan jaringan dan memperken alkan jalur dan akses jaringan yang tidak diinginkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 6	Bagaimana cara melindungi sumber daya komputasi Anda? Sumber daya komputasi di beban kerja Anda memerlukan beberapa lapisan pertahanan untuk membantu melindung i dari ancaman eksternal dan internal. Sumber daya komputasi mencakup EC2 instance, kontainer, fungsi AWS Lambda, layanan basis data, perangkat IoT, dan banyak lagi.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 6	Bagaimana cara melindungi sumber daya komputasi Anda? Sumber daya komputasi di beban kerja Anda memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman eksternal dan internal. Sumber daya komputasi mencakup EC2 instance, kontainer, fungsi AWS Lambda, layanan basis data, perangkat IoT, dan banyak lagi.	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 6	Bagaimana cara melindungi sumber daya komputasi Anda? Sumber daya komputasi di beban kerja Anda memerlukan beberapa lapisan pertahanan untuk membantu melindung i dari ancaman eksternal dan internal. Sumber daya komputasi mencakup EC2 instance, kontainer, fungsi AWS Lambda, layanan basis data, perangkat IoT, dan banyak lagi.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 6	Bagaimana cara melindungi sumber daya komputasi Anda? Sumber daya komputasi di beban kerja Anda memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman eksternal dan internal. Sumber daya komputasi mencakup EC2 instance, kontainer, fungsi AWS Lambda, layanan basis data, perangkat IoT, dan banyak lagi.	ec2- security-group-attached-to -eni-periodik	Aturan ini memastikan grup keamanan dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) atau ke ENI. Aturan ini membantu memantau kelompok keamanan yang tidak digunakan dalam inventaris dan pengelolaan lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 6	Bagaimana cara melindungi sumber daya komputasi Anda? Sumber daya komputasi di beban kerja Anda memerlukan beberapa lapisan pertahanan untuk membantu melindung i dari ancaman eksternal dan internal. Sumber daya komputasi mencakup EC2 instance, kontainer, fungsi AWS Lambda, layanan basis data, perangkat IoT, dan banyak lagi.	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 6	Bagaimana cara melindungi sumber daya komputasi Anda? Sumber daya komputasi di beban kerja Anda memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman eksternal dan internal. Sumber daya komputasi mencakup EC2 instance, kontainer, fungsi AWS Lambda, layanan basis data, perangkat IoT, dan banyak lagi.	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 6	Bagaimana cara melindungi sumber daya komputasi Anda? Sumber daya komputasi di beban kerja Anda memerlukan beberapa lapisan pertahanan untuk membantu melindungi dari ancaman eksternal dan internal. Sumber daya komputasi mencakup EC2 instance, kontainer, fungsi AWS Lambda, layanan basis data, perangkat IoT, dan banyak lagi.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi ke instans terkelola Anda dan memungkinkan Anda untuk menetapkan garis dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 6	Bagaimana cara melindungi sumber daya komputasi Anda? Sumber daya komputasi di beban kerja Anda memerlukan beberapa lapisan pertahanan untuk membantu melindung i dari ancaman eksternal dan internal. Sumber daya komputasi mencakup EC2 instance, kontainer, fungsi AWS Lambda, layanan basis data, perangkat IoT, dan banyak lagi.	ec2- -periksa managedinstance-pa tch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasika n beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	api-gw-cache-enabl ed-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasikan beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasikan beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	codebuild-project-artifact-encryption	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk AWS CodeBuild artefak Anda.
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasikan beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	codebuild-project-s3-log-terenkripsi	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk AWS CodeBuild log Anda yang disimpan di Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasikan beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasikan beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasikan beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasikan beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasikan beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasikan beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasikan beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasikan beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasikan beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasikan beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasikan beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasikan beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasikan beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasikan beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasikan beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasikan beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasikan beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasikan beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasikan beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasikan beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasikan beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasikan beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasikan beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasikan beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 8	Bagaimana cara melindungi data diam Anda? Lindungi data diam dengan mengimplementasikan beberapa kontrol, untuk mengurangi risiko akses tanpa otorisasi atau penanganan yang salah.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
DTK 9	Bagaimana cara melindungi data bergerak Anda? Lindungi data bergerak dengan mengimplementasikan beberapa kontrol untuk mengurangi risiko akses tanpa otorisasi atau hilangnya data.	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 9	Bagaimana cara melindungi data bergerak Anda? Lindungi data bergerak dengan mengimplementasikan beberapa kontrol untuk mengurangi risiko akses tanpa otorisasi atau hilangnya data.	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 9	Bagaimana cara melindungi data bergerak Anda? Lindungi data bergerak dengan mengimplementasikan beberapa kontrol untuk mengurangi risiko akses tanpa otorisasi atau hilangnya data.	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
DTK 9	Bagaimana cara melindungi data bergerak Anda? Lindungi data bergerak dengan mengimplementasikan beberapa kontrol untuk mengurangi risiko akses tanpa otorisasi atau hilangnya data.	alb-http-drop-invalid-header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 9	Bagaimana cara melindungi data bergerak Anda? Lindungi data bergerak dengan mengimplementasikan beberapa kontrol untuk mengurangi risiko akses tanpa otorisasi atau hilangnya data.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
DTK 9	Bagaimana cara melindungi data bergerak Anda? Lindungi data bergerak dengan mengimplementasikan beberapa kontrol untuk mengurangi risiko akses tanpa otorisasi atau hilangnya data.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 9	Bagaimana cara melindungi data bergerak Anda? Lindungi data bergerak dengan mengimplementasikan beberapa kontrol untuk mengurangi risiko akses tanpa otorisasi atau hilangnya data.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 9	Bagaimana cara melindungi data bergerak Anda? Lindungi data bergerak dengan mengimplementasikan beberapa kontrol untuk mengurangi risiko akses tanpa otorisasi atau hilangnya data.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
DTK 9	Bagaimana cara melindungi data bergerak Anda? Lindungi data bergerak dengan mengimplementasikan beberapa kontrol untuk mengurangi risiko akses tanpa otorisasi atau hilangnya data.	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 9	Bagaimana cara melindungi data bergerak Anda? Lindungi data bergerak dengan mengimplementasikan beberapa kontrol untuk mengurangi risiko akses tanpa otorisasi atau hilangnya data.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
DTK 9	Bagaimana cara melindungi data bergerak Anda? Lindungi data bergerak dengan mengimplementasikan beberapa kontrol untuk mengurangi risiko akses tanpa otorisasi atau hilangnya data.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 9	Bagaimana cara melindungi data bergerak Anda? Lindungi data bergerak dengan mengimplementasikan beberapa kontrol untuk mengurangi risiko akses tanpa otorisasi atau hilangnya data.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
DTK 9	Bagaimana cara melindungi data bergerak Anda? Lindungi data bergerak dengan mengimplementasikan beberapa kontrol untuk mengurangi risiko akses tanpa otorisasi atau hilangnya data.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DTK 9	Bagaimana cara melindungi data bergerak Anda? Lindungi data bergerak dengan mengimplementasikan beberapa kontrol untuk mengurangi risiko akses tanpa otorisasi atau hilangnya data.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Pilar Keamanan AWS Well-Architected.

Praktik Terbaik Operasional untuk BCP dan DR

Paket kesesuaian ini berisi AWS Config aturan berdasarkan BCP dan DR di dalamnya. AWS Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Operasional untuk BCP dan DR.

Praktik Terbaik Operasional untuk BNM T RMi

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara Manajemen Risiko Bank Negara Malaysia (BNM) dalam Teknologi (RMiT) dan aturan AWS Config yang dikelola. Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan berhubungan dengan satu atau beberapa kontrol BNM T RMi. Kontrol RMi T BNM dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.18	Lembaga keuangan harus melakukan uji tuntas dan mengevaluasi kontrol kriptografi yang terkait dengan teknologi yang digunakan untuk melindungi kerahasiaan, integritas, otentikasi, otorisasi, dan non-penolakan informasi. Apabila lembaga keuangan tidak menghasilkan kunci enkripsi sendiri, lembaga keuangan harus melakukan tindakan yang tepat	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	untuk memastikan kontrol dan proses yang kuat tersedia untuk mengelola kunci enkripsi. Apabila hal ini melibatkan ketergantungan pada penilaian pihak ketiga, lembaga keuangan harus mempertim bangkan apakah ketergantungan tersebut konsisten dengan selera risiko dan toleransi lembaga keuangan. Lembaga keuangan juga harus memperhatikan sumber daya sistem yang diperlukan untuk mendukung kontrol kriptografi dan risiko pengurangan visibilitas lalu lintas jaringan data yang telah dienkripsi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.18	Lembaga keuangan harus melakukan uji tuntas dan mengevaluasi kontrol kriptografi yang terkait dengan teknologi yang digunakan untuk melindungi kerahasiaan, integritas, otentikasi, otorisasi, dan non-penolakan informasi. Apabila lembaga keuangan tidak menghasilkan kunci enkripsi sendiri, lembaga keuangan harus melakukan tindakan yang tepat untuk memastikan kontrol dan proses yang kuat tersedia untuk mengelola kunci enkripsi. Apabila hal ini melibatkan ketergantungan pada penilaian pihak ketiga, lembaga keuangan harus mempertimbangkan apakah ketergantungan tersebut konsisten dengan selera risiko dan toleransi lembaga keuangan. Lembaga	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	keuangan juga harus memperhatikan sumber daya sistem yang diperlukan untuk mendukung kontrol kriptografi dan risiko pengurangan visibilitas lalu lintas jaringan data yang telah dienkripsi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.18	Lembaga keuangan harus melakukan uji tuntas dan mengevaluasi kontrol kriptografi yang terkait dengan teknologi yang digunakan untuk melindungi kerahasiaan, integritas, otentikasi, otorisasi, dan non-penolakan informasi. Apabila lembaga keuangan tidak menghasilkan kunci enkripsi sendiri, lembaga keuangan harus melakukan tindakan yang tepat untuk memastikan kontrol dan proses yang kuat tersedia untuk mengelola kunci enkripsi. Apabila hal ini melibatkan ketergantungan pada penilaian pihak ketiga, lembaga keuangan harus mempertimbangkan apakah ketergantungan tersebut konsisten dengan selera risiko dan toleransi lembaga keuangan. Lembaga	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	keuangan juga harus memperhatikan sumber daya sistem yang diperlukan untuk mendukung kontrol kriptografi dan risiko pengurangan visibilitas lalu lintas jaringan data yang telah dienkripsi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.18	Lembaga keuangan harus melakukan uji tuntas dan mengevaluasi kontrol kriptografi yang terkait dengan teknologi yang digunakan untuk melindungi kerahasiaan, integritas, otentikasi, otorisasi, dan non-penolakan informasi. Apabila lembaga keuangan tidak menghasilkan kunci enkripsi sendiri, lembaga keuangan harus melakukan tindakan yang tepat untuk memastikan kontrol dan proses yang kuat tersedia untuk mengelola kunci enkripsi. Apabila hal ini melibatkan ketergantungan pada penilaian pihak ketiga, lembaga keuangan harus mempertimbangkan apakah ketergantungan tersebut konsisten dengan selera risiko dan toleransi lembaga keuangan. Lembaga	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	keuangan juga harus memperhatikan sumber daya sistem yang diperlukan untuk mendukung kontrol kriptografi dan risiko pengurangan visibilitas lalu lintas jaringan data yang telah dienkripsi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.18	Lembaga keuangan harus melakukan uji tuntas dan mengevaluasi kontrol kriptografi yang terkait dengan teknologi yang digunakan untuk melindungi kerahasiaan, integritas, otentikasi, otorisasi, dan non-penolakan informasi. Apabila lembaga keuangan tidak menghasilkan kunci enkripsi sendiri, lembaga keuangan harus melakukan tindakan yang tepat untuk memastikan kontrol dan proses yang kuat tersedia untuk mengelola kunci enkripsi. Apabila hal ini melibatkan ketergantungan pada penilaian pihak ketiga, lembaga keuangan harus mempertimbangkan apakah ketergantungan tersebut konsisten dengan selera risiko dan toleransi lembaga keuangan. Lembaga	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	keuangan juga harus memperhatikan sumber daya sistem yang diperlukan untuk mendukung kontrol kriptografi dan risiko pengurangan visibilitas lalu lintas jaringan data yang telah dienkripsi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.18	Lembaga keuangan harus melakukan uji tuntas dan mengevaluasi kontrol kriptografi yang terkait dengan teknologi yang digunakan untuk melindungi kerahasiaan, integritas, otentikasi, otorisasi, dan non-penolakan informasi. Apabila lembaga keuangan tidak menghasilkan kunci enkripsi sendiri, lembaga keuangan harus melakukan tindakan yang tepat untuk memastikan kontrol dan proses yang kuat tersedia untuk mengelola kunci enkripsi. Apabila hal ini melibatkan ketergantungan pada penilaian pihak ketiga, lembaga keuangan harus mempertimbangkan apakah ketergantungan tersebut konsisten dengan selera risiko dan toleransi lembaga keuangan. Lembaga	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	keuangan juga harus memperhatikan sumber daya sistem yang diperlukan untuk mendukung kontrol kriptografi dan risiko pengurangan visibilitas lalu lintas jaringan data yang telah dienkripsi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.18	Lembaga keuangan harus melakukan uji tuntas dan mengevaluasi kontrol kriptografi yang terkait dengan teknologi yang digunakan untuk melindungi kerahasiaan, integritas, otentikasi, otorisasi, dan non-penolakan informasi. Apabila lembaga keuangan tidak menghasilkan kunci enkripsi sendiri, lembaga keuangan harus melakukan tindakan yang tepat untuk memastikan kontrol dan proses yang kuat tersedia untuk mengelola kunci enkripsi. Apabila hal ini melibatkan ketergantungan pada penilaian pihak ketiga, lembaga keuangan harus mempertimbangkan apakah ketergantungan tersebut konsisten dengan selera risiko dan toleransi lembaga keuangan. Lembaga	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	keuangan juga harus memperhatikan sumber daya sistem yang diperlukan untuk mendukung kontrol kriptografi dan risiko pengurangan visibilitas lalu lintas jaringan data yang telah dienkripsi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.18	Lembaga keuangan harus melakukan uji tuntas dan mengevaluasi kontrol kriptografi yang terkait dengan teknologi yang digunakan untuk melindungi kerahasiaan, integritas, otentikasi, otorisasi, dan non-penolakan informasi. Apabila lembaga keuangan tidak menghasilkan kunci enkripsi sendiri, lembaga keuangan harus melakukan tindakan yang tepat untuk memastikan kontrol dan proses yang kuat tersedia untuk mengelola kunci enkripsi. Apabila hal ini melibatkan ketergantungan pada penilaian pihak ketiga, lembaga keuangan harus mempertimbangkan apakah ketergantungan tersebut konsisten dengan selera risiko dan toleransi lembaga keuangan. Lembaga	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	keuangan juga harus memperhatikan sumber daya sistem yang diperlukan untuk mendukung kontrol kriptografi dan risiko pengurangan visibilitas lalu lintas jaringan data yang telah dienkripsi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.18	Lembaga keuangan harus melakukan uji tuntas dan mengevaluasi kontrol kriptografi yang terkait dengan teknologi yang digunakan untuk melindungi kerahasiaan, integritas, otentikasi, otorisasi, dan non-penolakan informasi. Apabila lembaga keuangan tidak menghasilkan kunci enkripsi sendiri, lembaga keuangan harus melakukan tindakan yang tepat untuk memastikan kontrol dan proses yang kuat tersedia untuk mengelola kunci enkripsi. Apabila hal ini melibatkan ketergantungan pada penilaian pihak ketiga, lembaga keuangan harus mempertimbangkan apakah ketergantungan tersebut konsisten dengan selera risiko dan toleransi lembaga keuangan. Lembaga	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	keuangan juga harus memperhatikan sumber daya sistem yang diperlukan untuk mendukung kontrol kriptografi dan risiko pengurangan visibilitas lalu lintas jaringan data yang telah dienkripsi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.18	Lembaga keuangan harus melakukan uji tuntas dan mengevaluasi kontrol kriptografi yang terkait dengan teknologi yang digunakan untuk melindungi kerahasiaan, integritas, otentikasi, otorisasi, dan non-penolakan informasi. Apabila lembaga keuangan tidak menghasilkan kunci enkripsi sendiri, lembaga keuangan harus melakukan tindakan yang tepat untuk memastikan kontrol dan proses yang kuat tersedia untuk mengelola kunci enkripsi. Apabila hal ini melibatkan ketergantungan pada penilaian pihak ketiga, lembaga keuangan harus mempertimbangkan apakah ketergantungan tersebut konsisten dengan selera risiko dan toleransi lembaga keuangan. Lembaga	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	keuangan juga harus memperhatikan sumber daya sistem yang diperlukan untuk mendukung kontrol kriptografi dan risiko pengurangan visibilitas lalu lintas jaringan data yang telah dienkripsi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.18	Lembaga keuangan harus melakukan uji tuntas dan mengevaluasi kontrol kriptografi yang terkait dengan teknologi yang digunakan untuk melindungi kerahasiaan, integritas, otentikasi, otorisasi, dan non-penolakan informasi. Apabila lembaga keuangan tidak menghasilkan kunci enkripsi sendiri, lembaga keuangan harus melakukan tindakan yang tepat untuk memastikan kontrol dan proses yang kuat tersedia untuk mengelola kunci enkripsi. Apabila hal ini melibatkan ketergantungan pada penilaian pihak ketiga, lembaga keuangan harus mempertimbangkan apakah ketergantungan tersebut konsisten dengan selera risiko dan toleransi lembaga keuangan. Lembaga	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	keuangan juga harus memperhatikan sumber daya sistem yang diperlukan untuk mendukung kontrol kriptografi dan risiko pengurangan visibilitas lalu lintas jaringan data yang telah dienkripsi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.18	Lembaga keuangan harus melakukan uji tuntas dan mengevaluasi kontrol kriptografi yang terkait dengan teknologi yang digunakan untuk melindungi kerahasiaan, integritas, otentikasi, otorisasi, dan non-penolakan informasi. Apabila lembaga keuangan tidak menghasilkan kunci enkripsi sendiri, lembaga keuangan harus melakukan tindakan yang tepat untuk memastikan kontrol dan proses yang kuat tersedia untuk mengelola kunci enkripsi. Apabila hal ini melibatkan ketergantungan pada penilaian pihak ketiga, lembaga keuangan harus mempertimbangkan apakah ketergantungan tersebut konsisten dengan selera risiko dan toleransi lembaga keuangan. Lembaga	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	keuangan juga harus memperhatikan sumber daya sistem yang diperlukan untuk mendukung kontrol kriptografi dan risiko pengurangan visibilitas lalu lintas jaringan data yang telah dienkripsi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.18	Lembaga keuangan harus melakukan uji tuntas dan mengevaluasi kontrol kriptografi yang terkait dengan teknologi yang digunakan untuk melindungi kerahasiaan, integritas, otentikasi, otorisasi, dan non-penolakan informasi. Apabila lembaga keuangan tidak menghasilkan kunci enkripsi sendiri, lembaga keuangan harus melakukan tindakan yang tepat untuk memastikan kontrol dan proses yang kuat tersedia untuk mengelola kunci enkripsi. Apabila hal ini melibatkan ketergantungan pada penilaian pihak ketiga, lembaga keuangan harus mempertimbangkan apakah ketergantungan tersebut konsisten dengan selera risiko dan toleransi lembaga keuangan. Lembaga	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	keuangan juga harus memperhatikan sumber daya sistem yang diperlukan untuk mendukung kontrol kriptografi dan risiko pengurangan visibilitas lalu lintas jaringan data yang telah dienkripsi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.18	Lembaga keuangan harus melakukan uji tuntas dan mengevaluasi kontrol kriptografi yang terkait dengan teknologi yang digunakan untuk melindungi kerahasiaan, integritas, otentikasi, otorisasi, dan non-penolakan informasi. Apabila lembaga keuangan tidak menghasilkan kunci enkripsi sendiri, lembaga keuangan harus melakukan tindakan yang tepat untuk memastikan kontrol dan proses yang kuat tersedia untuk mengelola kunci enkripsi. Apabila hal ini melibatkan ketergantungan pada penilaian pihak ketiga, lembaga keuangan harus mempertimbangkan apakah ketergantungan tersebut konsisten dengan selera risiko dan toleransi lembaga keuangan. Lembaga	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	keuangan juga harus memperhatikan sumber daya sistem yang diperlukan untuk mendukung kontrol kriptografi dan risiko pengurangan visibilitas lalu lintas jaringan data yang telah dienkripsi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.18	Lembaga keuangan harus melakukan uji tuntas dan mengevaluasi kontrol kriptografi yang terkait dengan teknologi yang digunakan untuk melindungi kerahasiaan, integritas, otentikasi, otorisasi, dan non-penolakan informasi. Apabila lembaga keuangan tidak menghasilkan kunci enkripsi sendiri, lembaga keuangan harus melakukan tindakan yang tepat untuk memastikan kontrol dan proses yang kuat tersedia untuk mengelola kunci enkripsi. Apabila hal ini melibatkan ketergantungan pada penilaian pihak ketiga, lembaga keuangan harus mempertimbangkan apakah ketergantungan tersebut konsisten dengan selera risiko dan toleransi lembaga keuangan. Lembaga	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	keuangan juga harus memperhatikan sumber daya sistem yang diperlukan untuk mendukung kontrol kriptografi dan risiko pengurangan visibilitas lalu lintas jaringan data yang telah dienkripsi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.18	Lembaga keuangan harus melakukan uji tuntas dan mengevaluasi kontrol kriptografi yang terkait dengan teknologi yang digunakan untuk melindungi kerahasiaan, integritas, otentikasi, otorisasi, dan non-penolakan informasi. Apabila lembaga keuangan tidak menghasilkan kunci enkripsi sendiri, lembaga keuangan harus melakukan tindakan yang tepat untuk memastikan kontrol dan proses yang kuat tersedia untuk mengelola kunci enkripsi. Apabila hal ini melibatkan ketergantungan pada penilaian pihak ketiga, lembaga keuangan harus mempertimbangkan apakah ketergantungan tersebut konsisten dengan selera risiko dan toleransi lembaga keuangan. Lembaga	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	keuangan juga harus memperhatikan sumber daya sistem yang diperlukan untuk mendukung kontrol kriptografi dan risiko pengurangan visibilitas lalu lintas jaringan data yang telah dienkripsi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.18	Lembaga keuangan harus melakukan uji tuntas dan mengevaluasi kontrol kriptografi yang terkait dengan teknologi yang digunakan untuk melindungi kerahasiaan, integritas, otentikasi, otorisasi, dan non-penolakan informasi. Apabila lembaga keuangan tidak menghasilkan kunci enkripsi sendiri, lembaga keuangan harus melakukan tindakan yang tepat untuk memastikan kontrol dan proses yang kuat tersedia untuk mengelola kunci enkripsi. Apabila hal ini melibatkan ketergantungan pada penilaian pihak ketiga, lembaga keuangan harus mempertimbangkan apakah ketergantungan tersebut konsisten dengan selera risiko dan toleransi lembaga keuangan. Lembaga	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	keuangan juga harus memperhatikan sumber daya sistem yang diperlukan untuk mendukung kontrol kriptografi dan risiko pengurangan visibilitas lalu lintas jaringan data yang telah dienkripsi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.18	Lembaga keuangan harus melakukan uji tuntas dan mengevaluasi kontrol kriptografi yang terkait dengan teknologi yang digunakan untuk melindungi kerahasiaan, integritas, otentikasi, otorisasi, dan non-penolakan informasi. Apabila lembaga keuangan tidak menghasilkan kunci enkripsi sendiri, lembaga keuangan harus melakukan tindakan yang tepat untuk memastikan kontrol dan proses yang kuat tersedia untuk mengelola kunci enkripsi. Apabila hal ini melibatkan ketergantungan pada penilaian pihak ketiga, lembaga keuangan harus mempertimbangkan apakah ketergantungan tersebut konsisten dengan selera risiko dan toleransi lembaga keuangan. Lembaga	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	keuangan juga harus memperhatikan sumber daya sistem yang diperlukan untuk mendukung kontrol kriptografi dan risiko pengurangan visibilitas lalu lintas jaringan data yang telah dienkripsi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.18	Lembaga keuangan harus melakukan uji tuntas dan mengevaluasi kontrol kriptografi yang terkait dengan teknologi yang digunakan untuk melindungi kerahasiaan, integritas, otentikasi, otorisasi, dan non-penolakan informasi. Apabila lembaga keuangan tidak menghasilkan kunci enkripsi sendiri, lembaga keuangan harus melakukan tindakan yang tepat untuk memastikan kontrol dan proses yang kuat tersedia untuk mengelola kunci enkripsi. Apabila hal ini melibatkan ketergantungan pada penilaian pihak ketiga, lembaga keuangan harus mempertimbangkan apakah ketergantungan tersebut konsisten dengan selera risiko dan toleransi lembaga keuangan. Lembaga	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	keuangan juga harus memperhatikan sumber daya sistem yang diperlukan untuk mendukung kontrol kriptografi dan risiko pengurangan visibilitas lalu lintas jaringan data yang telah dienkripsi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.18	Lembaga keuangan harus melakukan uji tuntas dan mengevaluasi kontrol kriptografi yang terkait dengan teknologi yang digunakan untuk melindungi kerahasiaan, integritas, otentikasi, otorisasi, dan non-penolakan informasi. Apabila lembaga keuangan tidak menghasilkan kunci enkripsi sendiri, lembaga keuangan harus melakukan tindakan yang tepat untuk memastikan kontrol dan proses yang kuat tersedia untuk mengelola kunci enkripsi. Apabila hal ini melibatkan ketergantungan pada penilaian pihak ketiga, lembaga keuangan harus mempertimbangkan apakah ketergantungan tersebut konsisten dengan selera risiko dan toleransi lembaga keuangan. Lembaga	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	keuangan juga harus memperhatikan sumber daya sistem yang diperlukan untuk mendukung kontrol kriptografi dan risiko pengurangan visibilitas lalu lintas jaringan data yang telah dienkripsi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.18	Lembaga keuangan harus melakukan uji tuntas dan mengevaluasi kontrol kriptografi yang terkait dengan teknologi yang digunakan untuk melindungi kerahasiaan, integritas, otentikasi, otorisasi, dan non-penolakan informasi. Apabila lembaga keuangan tidak menghasilkan kunci enkripsi sendiri, lembaga keuangan harus melakukan tindakan yang tepat untuk memastikan kontrol dan proses yang kuat tersedia untuk mengelola kunci enkripsi. Apabila hal ini melibatkan ketergantungan pada penilaian pihak ketiga, lembaga keuangan harus mempertimbangkan apakah ketergantungan tersebut konsisten dengan selera risiko dan toleransi lembaga keuangan. Lembaga	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	keuangan juga harus memperhatikan sumber daya sistem yang diperlukan untuk mendukung kontrol kriptografi dan risiko pengurangan visibilitas lalu lintas jaringan data yang telah dienkripsi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.18	Lembaga keuangan harus melakukan uji tuntas dan mengevaluasi kontrol kriptografi yang terkait dengan teknologi yang digunakan untuk melindungi kerahasiaan, integritas, otentikasi, otorisasi, dan non-penolakan informasi. Apabila lembaga keuangan tidak menghasilkan kunci enkripsi sendiri, lembaga keuangan harus melakukan tindakan yang tepat untuk memastikan kontrol dan proses yang kuat tersedia untuk mengelola kunci enkripsi. Apabila hal ini melibatkan ketergantungan pada penilaian pihak ketiga, lembaga keuangan harus mempertimbangkan apakah ketergantungan tersebut konsisten dengan selera risiko dan toleransi lembaga keuangan. Lembaga	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	keuangan juga harus memperhatikan sumber daya sistem yang diperlukan untuk mendukung kontrol kriptografi dan risiko pengurangan visibilitas lalu lintas jaringan data yang telah dienkripsi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.18	Lembaga keuangan harus melakukan uji tuntas dan mengevaluasi kontrol kriptografi yang terkait dengan teknologi yang digunakan untuk melindungi kerahasiaan, integritas, otentikasi, otorisasi, dan non-penolakan informasi. Apabila lembaga keuangan tidak menghasilkan kunci enkripsi sendiri, lembaga keuangan harus melakukan tindakan yang tepat untuk memastikan kontrol dan proses yang kuat tersedia untuk mengelola kunci enkripsi. Apabila hal ini melibatkan ketergantungan pada penilaian pihak ketiga, lembaga keuangan harus mempertimbangkan apakah ketergantungan tersebut konsisten dengan selera risiko dan toleransi lembaga keuangan. Lembaga	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	keuangan juga harus memperhatikan sumber daya sistem yang diperlukan untuk mendukung kontrol kriptografi dan risiko pengurangan visibilitas lalu lintas jaringan data yang telah dienkripsi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.18	Lembaga keuangan harus melakukan uji tuntas dan mengevaluasi kontrol kriptografi yang terkait dengan teknologi yang digunakan untuk melindungi kerahasiaan, integritas, otentikasi, otorisasi, dan non-penolakan informasi. Apabila lembaga keuangan tidak menghasilkan kunci enkripsi sendiri, lembaga keuangan harus melakukan tindakan yang tepat untuk memastikan kontrol dan proses yang kuat tersedia untuk mengelola kunci enkripsi. Apabila hal ini melibatkan ketergantungan pada penilaian pihak ketiga, lembaga keuangan harus mempertimbangkan apakah ketergantungan tersebut konsisten dengan selera risiko dan toleransi lembaga keuangan. Lembaga	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	keuangan juga harus memperhatikan sumber daya sistem yang diperlukan untuk mendukung kontrol kriptografi dan risiko pengurangan visibilitas lalu lintas jaringan data yang telah dienkripsi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.18	Lembaga keuangan harus melakukan uji tuntas dan mengevaluasi kontrol kriptografi yang terkait dengan teknologi yang digunakan untuk melindungi kerahasiaan, integritas, otentikasi, otorisasi, dan non-penolakan informasi. Apabila lembaga keuangan tidak menghasilkan kunci enkripsi sendiri, lembaga keuangan harus melakukan tindakan yang tepat untuk memastikan kontrol dan proses yang kuat tersedia untuk mengelola kunci enkripsi. Apabila hal ini melibatkan ketergantungan pada penilaian pihak ketiga, lembaga keuangan harus mempertimbangkan apakah ketergantungan tersebut konsisten dengan selera risiko dan toleransi lembaga keuangan. Lembaga	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	keuangan juga harus memperhatikan sumber daya sistem yang diperlukan untuk mendukung kontrol kriptografi dan risiko pengurangan visibilitas lalu lintas jaringan data yang telah dienkripsi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.18	Lembaga keuangan harus melakukan uji tuntas dan mengevaluasi kontrol kriptografi yang terkait dengan teknologi yang digunakan untuk melindungi kerahasiaan, integritas, otentikasi, otorisasi, dan non-penolakan informasi. Apabila lembaga keuangan tidak menghasilkan kunci enkripsi sendiri, lembaga keuangan harus melakukan tindakan yang tepat untuk memastikan kontrol dan proses yang kuat tersedia untuk mengelola kunci enkripsi. Apabila hal ini melibatkan ketergantungan pada penilaian pihak ketiga, lembaga keuangan harus mempertimbangkan apakah ketergantungan tersebut konsisten dengan selera risiko dan toleransi lembaga keuangan. Lembaga	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	keuangan juga harus memperhatikan sumber daya sistem yang diperlukan untuk mendukung kontrol kriptografi dan risiko pengurangan visibilitas lalu lintas jaringan data yang telah dienkripsi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.18	Lembaga keuangan harus melakukan uji tuntas dan mengevaluasi kontrol kriptografi yang terkait dengan teknologi yang digunakan untuk melindungi kerahasiaan, integritas, otentikasi, otorisasi, dan non-penolakan informasi. Apabila lembaga keuangan tidak menghasilkan kunci enkripsi sendiri, lembaga keuangan harus melakukan tindakan yang tepat untuk memastikan kontrol dan proses yang kuat tersedia untuk mengelola kunci enkripsi. Apabila hal ini melibatkan ketergantungan pada penilaian pihak ketiga, lembaga keuangan harus mempertimbangkan apakah ketergantungan tersebut konsisten dengan selera risiko dan toleransi lembaga keuangan. Lembaga	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	keuangan juga harus memperhatikan sumber daya sistem yang diperlukan untuk mendukung kontrol kriptografi dan risiko pengurangan visibilitas lalu lintas jaringan data yang telah dienkripsi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.18	Lembaga keuangan harus melakukan uji tuntas dan mengevaluasi kontrol kriptografi yang terkait dengan teknologi yang digunakan untuk melindungi kerahasiaan, integritas, otentikasi, otorisasi, dan non-penolakan informasi. Apabila lembaga keuangan tidak menghasilkan kunci enkripsi sendiri, lembaga keuangan harus melakukan tindakan yang tepat untuk memastikan kontrol dan proses yang kuat tersedia untuk mengelola kunci enkripsi. Apabila hal ini melibatkan ketergantungan pada penilaian pihak ketiga, lembaga keuangan harus mempertimbangkan apakah ketergantungan tersebut konsisten dengan selera risiko dan toleransi lembaga keuangan. Lembaga	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	keuangan juga harus memperhatikan sumber daya sistem yang diperlukan untuk mendukung kontrol kriptografi dan risiko pengurangan visibilitas lalu lintas jaringan data yang telah dienkripsi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.20	Lembaga keuangan harus menyimpan kunci kriptografi publik dalam sertifikat yang dikeluarkan oleh otoritas sertifikat yang sesuai dengan tingkat risiko. Sertifikat yang terkait dengan pelanggan harus dikeluarkan oleh otoritas sertifikat yang diakui. Lembaga keuangan harus memastikan bahwa implementasi protokol otentikasi dan tanda tangan menggunakan sertifikat tersebut tunduk pada perlindungan yang kuat untuk memastikan bahwa penggunaan kunci kriptografi pribadi yang sesuai dengan sertifikat pengguna mengikat secara hukum dan tidak dapat disangkal. Penerbitan awal dan perpanjangan sertifikat tersebut harus konsisten dengan praktik terbaik	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	industri dan spesifika si hukum/peraturan yang berlaku.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.20	Lembaga keuangan harus menyimpan kunci kriptografi publik dalam sertifika t yang dikeluarkan oleh otoritas sertifika t yang sesuai dengan tingkat risiko. Sertifika t yang terkait dengan pelanggan harus dikeluarkan oleh otoritas sertifikat yang diakui. Lembaga keuangan harus memastikan bahwa implementasi protokol otentikasi dan tanda tangan menggunak an sertifikat tersebut tunduk pada perlindun gan yang kuat untuk memastikan bahwa penggunaan kunci kriptografi pribadi yang sesuai dengan sertifikat pengguna mengikat secara hukum dan tidak dapat disangkal . Penerbitan awal dan perpanjangan sertifikat tersebut harus konsisten dengan praktik terbaik	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	industri dan spesifika si hukum/peraturan yang berlaku.		
10.27	Lembaga keuangan harus menetapka n mekanisme pemantauan waktu nyata untuk melacak pemanfaatan kapasitas dan kinerja proses dan layanan utama. Mekanisme pemantauan ini harus mampu memberika n peringatan yang tepat waktu dan dapat ditindaklanjuti kepada administrator.	autoscaling-group-elb-healthcheck-di perlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemelihar aan kapasitas dan ketersediaan yang memadai. Penyeimba ng beban secara berkala mengirimk an ping, mencoba koneksi, atau mengirim permintaa n untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scal ing. Jika instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.27	Lembaga keuangan harus menetapkan mekanisme pemantauan waktu nyata untuk melacak pemanfaatan kapasitas dan kinerja proses dan layanan utama. Mekanisme pemantauan ini harus mampu memberikan peringatan yang tepat waktu dan dapat ditindaklanjuti kepada administrator.	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.27	Lembaga keuangan harus menetapkan mekanisme pemantauan waktu nyata untuk melacak pemanfaatan kapasitas dan kinerja proses dan layanan utama. Mekanisme pemantauan ini harus mampu memberikan peringatan yang tepat waktu dan dapat ditindaklanjuti kepada administrator.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.27	Lembaga keuangan harus menetapkan mekanisme pemantauan waktu nyata untuk melacak pemanfaatan kapasitas dan kinerja proses dan layanan utama. Mekanisme pemantauan ini harus mampu memberikan peringatan yang tepat waktu dan dapat ditindaklanjuti kepada administrator.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.27	Lembaga keuangan harus menetapkan mekanisme pemantauan waktu nyata untuk melacak pemanfaatan kapasitas dan kinerja proses dan layanan utama. Mekanisme pemantauan ini harus mampu memberikan peringatan yang tepat waktu dan dapat ditindaklanjuti kepada administrator.	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
10.27	Lembaga keuangan harus menetapkan mekanisme pemantauan waktu nyata untuk melacak pemanfaatan kapasitas dan kinerja proses dan layanan utama. Mekanisme pemantauan ini harus mampu memberikan peringatan yang tepat waktu dan dapat ditindaklanjuti kepada administrator.	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.27	Lembaga keuangan harus menetapkan mekanisme pemantauan waktu nyata untuk melacak pemanfaatan kapasitas dan kinerja proses dan layanan utama. Mekanisme pemantauan ini harus mampu memberikan peringatan yang tepat waktu dan dapat ditindaklanjuti kepada administrator.	lambda-concurrency-check	Aturan ini memastikan bahwa batas tinggi dan rendah konkurensi fungsi Lambda ditetapkan. Ini dapat membantu dalam mendasarkan jumlah permintaan yang dilayani oleh fungsi Anda pada waktu tertentu.
10.27	Lembaga keuangan harus menetapkan mekanisme pemantauan waktu nyata untuk melacak pemanfaatan kapasitas dan kinerja proses dan layanan utama. Mekanisme pemantauan ini harus mampu memberikan peringatan yang tepat waktu dan dapat ditindaklanjuti kepada administrator.	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.27	Lembaga keuangan harus menetapkan mekanisme pemantauan waktu nyata untuk melacak pemanfaatan kapasitas dan kinerja proses dan layanan utama. Mekanisme pemantauan ini harus mampu memberikan peringatan yang tepat waktu dan dapat ditindaklanjuti kepada administrator.	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.34	Lembaga keuangan harus memastikan layanan jaringan untuk sistem kritisnya dapat diandalkan dan tidak memiliki SKOF untuk melindungi sistem kritis terhadap potensi kesalahan jaringan dan ancaman cyber.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.34	Lembaga keuangan harus memastikan layanan jaringan untuk sistem kritisnya dapat diandalkan dan tidak memiliki SKOF untuk melindungi sistem kritis terhadap potensi kesalahan jaringan dan ancaman cyber.	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.35	Lembaga keuangan harus menetapkan proses pemantauan bandwidth jaringan real-time dan metrik ketahanan layanan jaringan yang sesuai untuk menandai pemanfaat an bandwidth dan gangguan sistem yang berlebihan karena kemacetan bandwidth dan kesalahan jaringan. Ini termasuk analisis lalu lintas untuk mendeteksi tren dan anomali.	api-gw-xray-enabled	AWS X-Ray mengumpulkan data tentang permintaan yang disajikan aplikasi Anda, dan menyediak an alat yang dapat Anda gunakan untuk melihat, memfilter , dan mendapatkan wawasan tentang data tersebut guna mengidentifikasi masalah dan peluang pengoptimalan. Pastikan X-Ray diaktifkan sehingga Anda dapat melihat informasi terperinci tidak hanya tentang permintaan dan respons, tetapi juga tentang panggilan yang dilakukan aplikasi Anda ke AWS sumber daya hilir, layanan mikro, database, dan web HTTP. APIs

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.35	Lembaga keuangan harus menetapkan proses pemantauan bandwidth jaringan real-time dan metrik ketahanan layanan jaringan yang sesuai untuk menandai pemanfaat an bandwidth dan gangguan sistem yang berlebihan karena kemacetan bandwidth dan kesalahan jaringan. Ini termasuk analisis lalu lintas untuk mendeteksi tren dan anomali.	cloudwatch-alarm-a ction-check	Amazon CloudWatc h mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasark an pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActi onRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.35	Lembaga keuangan harus menetapkan proses pemantauan bandwidth jaringan real-time dan metrik ketahanan layanan jaringan yang sesuai untuk menandai pemanfaat an bandwidth dan gangguan sistem yang berlebihan karena kemacetan bandwidth dan kesalahan jaringan. Ini termasuk analisis lalu lintas untuk mendeteksi tren dan anomali.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.35	Lembaga keuangan harus menetapkan proses pemantauan bandwidth jaringan real-time dan metrik ketahanan layanan jaringan yang sesuai untuk menandai pemanfaat an bandwidth dan gangguan sistem yang berlebihan karena kemacetan bandwidth dan kesalahan jaringan. Ini termasuk analisis lalu lintas untuk mendeteksi tren dan anomali.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.36	Lembaga keuangan harus memastikan layanan jaringan yang mendukung sistem kritis dirancang dan diimplementasikan untuk memastikan kerahasiaan, integrita s, dan ketersediaan data.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
10.36	Lembaga keuangan harus memastikan layanan jaringan yang mendukung sistem kritis dirancang dan diimplementasikan untuk memastikan kerahasiaan, integrita s, dan ketersediaan data.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.36	Lembaga keuangan harus memastikan layanan jaringan yang mendukung sistem kritis dirancang dan diimplementasikan untuk memastikan kerahasiaan, integrita s, dan ketersediaan data.	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
10.36	Lembaga keuangan harus memastikan layanan jaringan yang mendukung sistem kritis dirancang dan diimplementasikan untuk memastikan kerahasiaan, integrita s, dan ketersediaan data.	elb-deletion-prote ction-enabled	Aturan ini memastika n bahwa Elastic Load Balancing memiliki perlindun gan penghapus an yang diaktifka n. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersedi aan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.36	Lembaga keuangan harus memastikan layanan jaringan yang mendukung sistem kritis dirancang dan diimplementasikan untuk memastikan kerahasiaan, integrita s, dan ketersediaan data.	nlb-cross-zone-loa d-menyeimbangkan diaktifkan	Aktifkan penyeimba ngan beban lintas zona untuk Network Load Balancers (NLBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimba ngan beban lintas zona mengurang i kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkat kan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.38	Lembaga keuangan harus memastikan log perangkat jaringan yang memadai dan relevan disimpan untuk penyelidikan dan tujuan forensik setidaknya selama tiga tahun.	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktifkan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengotentikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediakan sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna IAM adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna IAM. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna IAM.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsageUsia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapka n perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilik an saat menggunak an layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositori data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.51	Lembaga keuangan harus menerapkan perlindungan yang tepat terhadap informasi pelanggan dan pihak lawan serta data kepemilikan saat menggunakan layanan cloud untuk melindungi dari pengungkapan dan akses yang tidak sah. Ini harus mencakup mempertahankan kepemilikan, kontrol dan pengelolaan semua data yang berkaitan dengan informasi pelanggan dan rekanan, data kepemilikan dan layanan yang dihosting di cloud, termasuk manajemen kunci kriptografi yang relevan.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.52	Lembaga keuangan harus menerapkan kebijakan kontrol akses yang sesuai untuk identifikasi, otentikasi, dan otorisasi pengguna (pengguna internal dan eksternal seperti penyedia layanan pihak ketiga). Ini harus mengatasi kontrol akses teknologi logis dan fisik yang sepadan dengan tingkat risiko akses tidak sah ke sistem teknologinya.	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.52	Lembaga keuangan harus menerapkan kebijakan kontrol akses yang sesuai untuk identifikasi, otentikasi, dan otorisasi pengguna (pengguna internal dan eksternal seperti penyedia layanan pihak ketiga). Ini harus mengatasi kontrol akses teknologi logis dan fisik yang sepadan dengan tingkat risiko akses tidak sah ke sistem teknologinya.	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.52	Lembaga keuangan harus menerapkan kebijakan kontrol akses yang sesuai untuk identifikasi, otentikasi, dan otorisasi pengguna (pengguna internal dan eksternal seperti penyedia layanan pihak ketiga). Ini harus mengatasi kontrol akses teknologi logis dan fisik yang sepadan dengan tingkat risiko akses tidak sah ke sistem teknologinya.	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.52	Lembaga keuangan harus menerapkan kebijakan kontrol akses yang sesuai untuk identifikasi, otentikasi, dan otorisasi pengguna (pengguna internal dan eksternal seperti penyedia layanan pihak ketiga). Ini harus mengatasi kontrol akses teknologi logis dan fisik yang sepadan dengan tingkat risiko akses tidak sah ke sistem teknologinya.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktifkan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengotentikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediakan sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.52	Lembaga keuangan harus menerapka n kebijakan kontrol akses yang sesuai untuk identifikasi, otentikasi, dan otorisasi pengguna (pengguna internal dan eksternal seperti penyedia layanan pihak ketiga). Ini harus mengatasi kontrol akses teknologi logis dan fisik yang sepadan dengan tingkat risiko akses tidak sah ke sistem teknologinya.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
10.52	Lembaga keuangan harus menerapkan kebijakan kontrol akses yang sesuai untuk identifikasi, otentikasi, dan otorisasi pengguna (pengguna internal dan eksternal seperti penyedia layanan pihak ketiga). Ini harus mengatasi kontrol akses teknologi logis dan fisik yang sepadan dengan tingkat risiko akses tidak sah ke sistem teknologinya.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.52	Lembaga keuangan harus menerapkan kebijakan kontrol akses yang sesuai untuk identifikasi, otentikasi, dan otorisasi pengguna (pengguna internal dan eksternal seperti penyedia layanan pihak ketiga). Ini harus mengatasi kontrol akses teknologi logis dan fisik yang sepadan dengan tingkat risiko akses tidak sah ke sistem teknologinya.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.52	Lembaga keuangan harus menerapkan kebijakan kontrol akses yang sesuai untuk identifikasi, otentikasi, dan otorisasi pengguna (pengguna internal dan eksternal seperti penyedia layanan pihak ketiga). Ini harus mengatasi kontrol akses teknologi logis dan fisik yang sepadan dengan tingkat risiko akses tidak sah ke sistem teknologinya.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.52	Lembaga keuangan harus menerapka n kebijakan kontrol akses yang sesuai untuk identifikasi, otentikasi, dan otorisasi pengguna (pengguna internal dan eksternal seperti penyedia layanan pihak ketiga). Ini harus mengatasi kontrol akses teknologi logis dan fisik yang sepadan dengan tingkat risiko akses tidak sah ke sistem teknologinya.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.52	Lembaga keuangan harus menerapkan kebijakan kontrol akses yang sesuai untuk identifikasi, otentikasi, dan otorisasi pengguna (pengguna internal dan eksternal seperti penyedia layanan pihak ketiga). Ini harus mengatasi kontrol akses teknologi logis dan fisik yang sepadan dengan tingkat risiko akses tidak sah ke sistem teknologinya.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna IAM adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.52	Lembaga keuangan harus menerapkan kebijakan kontrol akses yang sesuai untuk identifikasi, otentikasi, dan otorisasi pengguna (pengguna internal dan eksternal seperti penyedia layanan pihak ketiga). Ini harus mengatasi kontrol akses teknologi logis dan fisik yang sepadan dengan tingkat risiko akses tidak sah ke sistem teknologinya.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna IAM. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna IAM.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.52	Lembaga keuangan harus menerapkan kebijakan kontrol akses yang sesuai untuk identifikasi, otentikasi, dan otorisasi pengguna (pengguna internal dan eksternal seperti penyedia layanan pihak ketiga). Ini harus mengatasi kontrol akses teknologi logis dan fisik yang sepadan dengan tingkat risiko akses tidak sah ke sistem teknologinya.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.52	Lembaga keuangan harus menerapkan kebijakan kontrol akses yang sesuai untuk identifikasi, otentikasi, dan otorisasi pengguna (pengguna internal dan eksternal seperti penyedia layanan pihak ketiga). Ini harus menangani kontrol akses teknologi logis dan fisik yang sepadan dengan tingkat risiko akses tidak sah ke sistem teknologinya.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsageUsia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.52	Lembaga keuangan harus menerapkan kebijakan kontrol akses yang sesuai untuk identifikasi, otentikasi, dan otorisasi pengguna (pengguna internal dan eksternal seperti penyedia layanan pihak ketiga). Ini harus mengatasi kontrol akses teknologi logis dan fisik yang sepadan dengan tingkat risiko akses tidak sah ke sistem teknologinya.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.52	Lembaga keuangan harus menerapkan kebijakan kontrol akses yang sesuai untuk identifikasi, otentikasi, dan otorisasi pengguna (pengguna internal dan eksternal seperti penyedia layanan pihak ketiga). Ini harus mengatasi kontrol akses teknologi logis dan fisik yang sepadan dengan tingkat risiko akses tidak sah ke sistem teknologinya.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.53 (b) (h) (i)	Dalam mengamati paragraf 10.52, lembaga keuangan harus mempertim bangkan prinsip-prinsip berikut dalam kebijakan kontrol aksesnya: (b) menggunakan hak akses “hak istimewa terkecil” atau atas dasar 'need-to-have' di mana hanya izin minimum yang cukup diberikan kepada pengguna yang sah untuk menjalank an peran mereka; (h) membatasi dan mengontro l pembagian ID pengguna dan kata sandi di beberapa pengguna; dan (i) mengontrol penggunaan konvensi penamaan ID pengguna generik demi identitas yang lebih pribadi bisa dimengerti. IDs	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.53 (b)	Dalam mengamati paragraf 10.52, lembaga keuangan harus mempertim bangkan prinsip-prinsip berikut dalam kebijakan kontrol aksesnya: (b) menggunakan hak akses “hak istimewa terkecil” atau atas dasar 'need-to-have' di mana hanya izin minimum yang cukup diberikan kepada pengguna yang sah untuk menjalankan peran mereka;	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.53 (b)	Dalam mengamati paragraf 10.52, lembaga keuangan harus mempertim bangkan prinsip-prinsip berikut dalam kebijakan kontrol aksesnya: (b) menggunakan hak akses “hak istimewa terkecil” atau atas dasar 'need-to-have' di mana hanya izin minimum yang cukup diberikan kepada pengguna yang sah untuk menjalankan peran mereka;	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengotent ikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.53 (b)	Dalam mengamati paragraf 10.52, lembaga keuangan harus mempertim bangkan prinsip-prinsip berikut dalam kebijakan kontrol aksesnya: (b) menggunakan hak akses “hak istimewa terkecil” atau atas dasar 'need-to-have' di mana hanya izin minimum yang cukup diberikan kepada pengguna yang sah untuk menjalankan peran mereka;	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
10.53 (b)	Dalam mengamati paragraf 10.52, lembaga keuangan harus mempertim bangkan prinsip-prinsip berikut dalam kebijakan kontrol aksesnya: (b) menggunakan hak akses “hak istimewa terkecil” atau atas dasar 'need-to-have' di mana hanya izin minimum yang cukup diberikan kepada pengguna yang sah untuk menjalankan peran mereka;	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.53 (b)	Dalam mengamati paragraf 10.52, lembaga keuangan harus mempertim bangkan prinsip-prinsip berikut dalam kebijakan kontrol aksesnya: (b) menggunakan hak akses “hak istimewa terkecil” atau atas dasar 'need-to-have' di mana hanya izin minimum yang cukup diberikan kepada pengguna yang sah untuk menjalankan peran mereka;	iam-policy-no-statements-with-admin-access	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.53 (b)	Dalam mengamati paragraf 10.52, lembaga keuangan harus mempertim bangkan prinsip-prinsip berikut dalam kebijakan kontrol aksesnya: (b) menggunakan hak akses “hak istimewa terkecil” atau atas dasar 'need-to-have' di mana hanya izin minimum yang cukup diberikan kepada pengguna yang sah untuk menjalankan peran mereka;	iam-user-group-membership-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna IAM adalah anggota setidaknya satu grup. Mengizink an pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.53 (b)	Dalam mengamati paragraf 10.52, lembaga keuangan harus mempertim bangkan prinsip-prinsip berikut dalam kebijakan kontrol aksesnya: (b) menggunakan hak akses “hak istimewa terkecil” atau atas dasar 'need-to-have' di mana hanya izin minimum yang cukup diberikan kepada pengguna yang sah untuk menjalankan peran mereka;	iam-user-no-policies-periksa	Aturan ini memastika n kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapka n hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.53 (c) (f)	Dalam mengamati paragraf 10.52, lembaga keuangan harus mempertim bangkan prinsip-prinsip berikut dalam kebijakan kontrol aksesnya: (c) menggunakan hak akses terikat waktu yang membatasi akses ke periode tertentu termasuk hak akses yang diberikan kepada penyedia layanan; (f) mengadopsi otentikas i yang lebih kuat untuk kegiatan penting termasuk untuk akses jarak jauh	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifik asi berdasark an kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkin kan Anda untuk mengatur secara opsional RequireUp percaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.53 (f) (h)	Dalam mengamati paragraf 10.52, lembaga keuangan harus mempertim bangkan prinsip-prinsip berikut dalam kebijakan kontrol aksesnya: (f) mengadopsi otentikasi yang lebih kuat untuk kegiatan penting termasuk untuk akses jarak jauh; (h) membatasi dan mengontro l pembagian ID pengguna dan kata sandi di beberapa pengguna	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastika n otentikasi multi-fak tor (MFA) diaktifka n untuk semua pengguna IAM. MFA menambahk an lapisan perlindun gan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna IAM.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.53 (f) (h)	Dalam mengamati paragraf 10.54, lembaga keuangan harus mempertim bangkan prinsip-prinsip berikut dalam kebijakan kontrol aksesnya: (f) mengadopsi otentikasi yang lebih kuat untuk kegiatan penting termasuk untuk akses jarak jauh; (h) membatasi dan mengontro l pembagian ID pengguna dan kata sandi di beberapa pengguna	root-account-hardw are-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindun gan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.53 (f) (h)	Dalam mengamati paragraf 10.54, lembaga keuangan harus mempertim bangkan prinsip-prinsip berikut dalam kebijakan kontrol aksesnya: (f) mengadopsi otentikasi yang lebih kuat untuk kegiatan penting termasuk untuk akses jarak jauh; (h) membatasi dan mengontro l pembagian ID pengguna dan kata sandi di beberapa pengguna	root-account-mfa-e nabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindun gan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.54	Lembaga keuangan harus menggunakan proses otentikasi yang kuat untuk memastikan keaslian identitas yang digunakan. Mekanisme otentikasi harus sepadan dengan kekritisan fungsi dan mengadopsi setidaknya satu atau lebih dari tiga faktor otentikasi dasar ini, yaitu, sesuatu yang diketahui pengguna (misalnya kata sandi, PIN), sesuatu yang dimiliki pengguna (misalnya kartu pintar, perangkat keamanan) dan sesuatu yang pengguna (misalnya karakteristik biometrik, seperti sidik jari atau pola retina).	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna IAM. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna IAM.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.54	Lembaga keuangan harus menggunakan proses otentikasi yang kuat untuk memastikan keaslian identitas yang digunakan. Mekanisme otentikasi harus sepadan dengan kekritisan fungsi dan mengadopsi setidaknya satu atau lebih dari tiga faktor otentikasi dasar ini, yaitu, sesuatu yang diketahui pengguna (misalnya kata sandi, PIN), sesuatu yang dimiliki pengguna (misalnya kartu pintar, perangkat keamanan) dan sesuatu yang pengguna (misalnya karakteristik biometrik, seperti sidik jari atau pola retina).	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.54	Lembaga keuangan harus menggunakan proses otentikasi yang kuat untuk memastikan keaslian identitas yang digunakan. Mekanisme otentikasi harus sepadan dengan kekritisan fungsi dan mengadopsi setidaknya satu atau lebih dari tiga faktor otentikasi dasar ini, yaitu, sesuatu yang diketahui pengguna (misalnya kata sandi, PIN), sesuatu yang dimiliki pengguna (misalnya kartu pintar, perangkat keamanan) dan sesuatu yang pengguna (misalnya karakteristik biometrik, seperti sidik jari atau pola retina).	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.55	Lembaga keuangan harus secara berkala meninjau dan menyesuaikan praktik kata sandinya untuk meningkatkan ketahanan terhadap serangan yang terus berkembang. Ini termasuk pembuatan kata sandi yang efektif dan aman. Harus ada kontrol yang tepat untuk memeriksa kekuatan kata sandi yang dibuat.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.56	Metode otentikasi yang bergantung pada lebih dari satu faktor biasanya lebih sulit dikompromikan daripada sistem faktor tunggal. Mengingat hal ini, lembaga keuangan didorong untuk merancang dan menerapkan dengan benar (terutama dalam sistem berisiko tinggi atau 'sistem masuk tunggal') otentikasi multi-faktor (MFA) yang lebih andal dan memberikan pencegah penipuan yang lebih kuat.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna IAM. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna IAM.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.56	Metode otentikasi yang bergantung pada lebih dari satu faktor biasanya lebih sulit dikompromikan daripada sistem faktor tunggal. Mengingat hal ini, lembaga keuangan didorong untuk merancang dan menerapkan dengan benar (terutama dalam sistem berisiko tinggi atau 'sistem masuk tunggal') otentikasi multi-faktor (MFA) yang lebih andal dan memberikan pencegah penipuan yang lebih kuat.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.56	Metode otentikasi yang bergantung pada lebih dari satu faktor biasanya lebih sulit dikompromikan daripada sistem faktor tunggal. Mengingat hal ini, lembaga keuangan didorong untuk merancang dan menerapkan dengan benar (terutama dalam sistem berisiko tinggi atau 'sistem masuk tunggal') otentikasi multi-faktor (MFA) yang lebih andal dan memberikan pencegah penipuan yang lebih kuat.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.59	Lembaga keuangan harus memastika n (a) kontrol akses ke sistem di seluruh perusahaan dikelola dan dipantau secara efektif; dan (b) aktivitas pengguna dalam sistem kritis dicatat untuk audit dan investigasi. Log aktivitas harus dipelihara setidaknya selama tiga tahun dan ditinjau secara teratur tepat waktu.	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastika n kunci akses IAM diputar sebagaima na ditentukan oleh kebijakan organisas i. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurang i dampak bisnis jika kunci dikompromikan. Aturan ini memerluka n nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.59	Lembaga keuangan harus memastikan (a) kontrol akses ke sistem di seluruh perusahaan dikelola dan dipantau secara efektif; dan (b) aktivitas pengguna dalam sistem kritis dicatat untuk audit dan investigasi. Log aktivitas harus dipelihara setidaknya selama tiga tahun dan ditinjau secara teratur tepat waktu.	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.
10.59	Lembaga keuangan harus memastikan (a) kontrol akses ke sistem di seluruh perusahaan dikelola dan dipantau secara efektif; dan (b) aktivitas pengguna dalam sistem kritis dicatat untuk audit dan investigasi. Log aktivitas harus dipelihara setidaknya selama tiga tahun dan ditinjau secara teratur tepat waktu.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.59	Lembaga keuangan harus memastikan (a) kontrol akses ke sistem di seluruh perusahaan dikelola dan dipantau secara efektif; dan (b) aktivitas pengguna dalam sistem kritis dicatat untuk audit dan investigasi. Log aktivitas harus dipelihara setidaknya selama tiga tahun dan ditinjau secara teratur tepat waktu.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
10.59	Lembaga keuangan harus memastikan (a) kontrol akses ke sistem di seluruh perusahaan dikelola dan dipantau secara efektif; dan (b) aktivitas pengguna dalam sistem kritis dicatat untuk audit dan investigasi. Log aktivitas harus dipelihara setidaknya selama tiga tahun dan ditinjau secara teratur tepat waktu.	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.59	Lembaga keuangan harus memastika n (a) kontrol akses ke sistem di seluruh perusahaan dikelola dan dipantau secara efektif; dan (b) aktivitas pengguna dalam sistem kritis dicatat untuk audit dan investigasi. Log aktivitas harus dipelihara setidaknya selama tiga tahun dan ditinjau secara teratur tepat waktu.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
10.59	Lembaga keuangan harus memastika n (a) kontrol akses ke sistem di seluruh perusahaan dikelola dan dipantau secara efektif; dan (b) aktivitas pengguna dalam sistem kritis dicatat untuk audit dan investigasi. Log aktivitas harus dipelihara setidaknya selama tiga tahun dan ditinjau secara teratur tepat waktu.	cw-loggroup-retent ion-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonst ruksi dan mengident ifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.59	Lembaga keuangan harus memastika n (a) kontrol akses ke sistem di seluruh perusahaan dikelola dan dipantau secara efektif; dan (b) aktivitas pengguna dalam sistem kritis dicatat untuk audit dan investigasi. Log aktivitas harus dipelihara setidaknya selama tiga tahun dan ditinjau secara teratur tepat waktu.	ec2- instance-profile-a ttached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirk an profil instans ke instans Anda dapat membantu pengelola an hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.59	Lembaga keuangan harus memastika n (a) kontrol akses ke sistem di seluruh perusahaan dikelola dan dipantau secara efektif; dan (b) aktivitas pengguna dalam sistem kritis dicatat untuk audit dan investigasi. Log aktivitas harus dipelihara setidaknya selama tiga tahun dan ditinjau secara teratur tepat waktu.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.59	Lembaga keuangan harus memastika n (a) kontrol akses ke sistem di seluruh perusahaan dikelola dan dipantau secara efektif; dan (b) aktivitas pengguna dalam sistem kritis dicatat untuk audit dan investigasi. Log aktivitas harus dipelihara setidaknya selama tiga tahun dan ditinjau secara teratur tepat waktu.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.59	Lembaga keuangan harus memastika n (a) kontrol akses ke sistem di seluruh perusahaan dikelola dan dipantau secara efektif; dan (b) aktivitas pengguna dalam sistem kritis dicatat untuk audit dan investigasi. Log aktivitas harus dipelihara setidaknya selama tiga tahun dan ditinjau secara teratur tepat waktu.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifik asi berdasark an kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkin kan Anda untuk mengatur secara opsional RequireUp percaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.59	Lembaga keuangan harus memastika n (a) kontrol akses ke sistem di seluruh perusahaan dikelola dan dipantau secara efektif; dan (b) aktivitas pengguna dalam sistem kritis dicatat untuk audit dan investigasi. Log aktivitas harus dipelihara setidaknya selama tiga tahun dan ditinjau secara teratur tepat waktu.	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.59	Lembaga keuangan harus memastika n (a) kontrol akses ke sistem di seluruh perusahaan dikelola dan dipantau secara efektif; dan (b) aktivitas pengguna dalam sistem kritis dicatat untuk audit dan investigasi. Log aktivitas harus dipelihara setidaknya selama tiga tahun dan ditinjau secara teratur tepat waktu.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.59	Lembaga keuangan harus memastika n (a) kontrol akses ke sistem di seluruh perusahaan dikelola dan dipantau secara efektif; dan (b) aktivitas pengguna dalam sistem kritis dicatat untuk audit dan investigasi. Log aktivitas harus dipelihara setidaknya selama tiga tahun dan ditinjau secara teratur tepat waktu.	iam-user-group-membership-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna IAM adalah anggota setidaknya satu grup. Mengizink an pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.59	Lembaga keuangan harus memastikan (a) kontrol akses ke sistem di seluruh perusahaan dikelola dan dipantau secara efektif; dan (b) aktivitas pengguna dalam sistem kritis dicatat untuk audit dan investigasi. Log aktivitas harus dipelihara setidaknya selama tiga tahun dan ditinjau secara teratur tepat waktu.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.59	Lembaga keuangan harus memastikan (a) kontrol akses ke sistem di seluruh perusahaan dikelola dan dipantau secara efektif; dan (b) aktivitas pengguna dalam sistem kritis dicatat untuk audit dan investigasi. Log aktivitas harus dipelihara setidaknya selama tiga tahun dan ditinjau secara teratur tepat waktu.	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.59	Lembaga keuangan harus memastika n (a) kontrol akses ke sistem di seluruh perusahaan dikelola dan dipantau secara efektif; dan (b) aktivitas pengguna dalam sistem kritis dicatat untuk audit dan investigasi. Log aktivitas harus dipelihara setidaknya selama tiga tahun dan ditinjau secara teratur tepat waktu.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.59	Lembaga keuangan harus memastikan (a) kontrol akses ke sistem di seluruh perusahaan dikelola dan dipantau secara efektif; dan (b) aktivitas pengguna dalam sistem kritis dicatat untuk audit dan investigasi. Log aktivitas harus dipelihara setidaknya selama tiga tahun dan ditinjau secara teratur tepat waktu.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.59	Lembaga keuangan harus memastika n (a) kontrol akses ke sistem di seluruh perusahaan dikelola dan dipantau secara efektif; dan (b) aktivitas pengguna dalam sistem kritis dicatat untuk audit dan investigasi. Log aktivitas harus dipelihara setidaknya selama tiga tahun dan ditinjau secara teratur tepat waktu.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediak an metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinc i untuk permintaa n yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.59	Lembaga keuangan harus memastika n (a) kontrol akses ke sistem di seluruh perusahaan dikelola dan dipantau secara efektif; dan (b) aktivitas pengguna dalam sistem kritis dicatat untuk audit dan investigasi. Log aktivitas harus dipelihara setidaknya selama tiga tahun dan ditinjau secara teratur tepat waktu.	wafv2-logging-diak tifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatata n AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.60	Dalam memenuhi persyaratan berdasarkan paragraf 10.59, lembaga keuangan besar diharuskan untuk (a) menyebarkan sistem manajemen akses identitas untuk mengelola dan memantau akses pengguna ke sistem perusahaan secara efektif; dan (b) menyebarkan alat audit otomatis untuk menandai anomali apa pun.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.60	Dalam memenuhi persyaratan berdasarkan paragraf 10.61, lembaga keuangan besar diharuskan untuk (a) menyebarkan sistem manajemen akses identitas untuk mengelola dan memantau akses pengguna ke sistem perusahaan secara efektif; dan (b) menyebarkan alat audit otomatis untuk menandai anomali apa pun.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.60	Dalam memenuhi persyaratan berdasarkan paragraf 10.61, lembaga keuangan besar diharuskan untuk (a) menyebarkan sistem manajemen akses identitas untuk mengelola dan memantau akses pengguna ke sistem perusahaan secara efektif; dan (b) menyebarkan alat audit otomatis untuk menandai anomali apa pun.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.61	Lembaga keuangan harus memastikan bahwa sistem kritis tidak berjalan pada sistem yang sudah ketinggalan zaman dengan kerentana n keamanan yang diketahui atau sistem teknologi end-of-life (EOL). Dalam hal ini, lembaga keuangan harus secara jelas menetapkan tanggung jawab untuk fungsi yang diidentifikasi: (a) untuk terus memantau dan menerapkan rilis patch terbaru secara tepat waktu; dan (b) mengident ifikasi sistem teknologi kritis yang mendekati EOL untuk tindakan perbaikan lebih lanjut.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.61	Lembaga keuangan harus memastikan bahwa sistem kritis tidak berjalan pada sistem yang sudah ketinggalan zaman dengan kerentana n keamanan yang diketahui atau sistem teknologi end-of-life (EOL). Dalam hal ini, lembaga keuangan harus secara jelas menetapkan tanggung jawab untuk fungsi yang diidentifikasi: (a) untuk terus memantau dan menerapkan rilis patch terbaru secara tepat waktu; dan (b) mengident ifikasi sistem teknologi kritis yang mendekati EOL untuk tindakan perbaikan lebih lanjut.	ec2- -periksa managedinstance-as sociation-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventari s platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.61	Lembaga keuangan harus memastikan bahwa sistem kritis tidak berjalan pada sistem yang sudah ketinggalan zaman dengan kerentana n keamanan yang diketahui atau sistem teknologi end-of-life (EOL). Dalam hal ini, lembaga keuangan harus secara jelas menetapkan tanggung jawab untuk fungsi yang diidentifikasi: (a) untuk terus memantau dan menerapkan rilis patch terbaru secara tepat waktu; dan (b) mengident ifikasi sistem teknologi kritis yang mendekati EOL untuk tindakan perbaikan lebih lanjut.	ec2- -periksa managedinstance-pa tch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.61	Lembaga keuangan harus memastikan bahwa sistem kritis tidak berjalan pada sistem yang sudah ketinggalan zaman dengan kerentana n keamanan yang diketahui atau sistem teknologi end-of-life (EOL). Dalam hal ini, lembaga keuangan harus secara jelas menetapkan tanggung jawab untuk fungsi yang diidentifikasi: (a) untuk terus memantau dan menerapkan rilis patch terbaru secara tepat waktu; dan (b) mengident ifikasi sistem teknologi kritis yang mendekati EOL untuk tindakan perbaikan lebih lanjut.	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.61	Lembaga keuangan harus memastikan bahwa sistem kritis tidak berjalan pada sistem yang sudah ketinggalan zaman dengan kerentana n keamanan yang diketahui atau sistem teknologi end-of-life (EOL). Dalam hal ini, lembaga keuangan harus secara jelas menetapkan tanggung jawab untuk fungsi yang diidentifikasi: (a) untuk terus memantau dan menerapkan rilis patch terbaru secara tepat waktu; dan (b) mengident ifikasi sistem teknologi kritis yang mendekati EOL untuk tindakan perbaikan lebih lanjut.	redshift-cluster-m aintenancesettings-check	Aturan ini memastika n bahwa klaster Amazon Redshift memiliki pengatura n yang diinginka n untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemelihar aan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrad e. Bawaannya adalah benar. Ini juga memungkin kan Anda secara opsional mengatur preferredMaintenan ceWindow (defaultn ya adalah sat: 16:00 -sat: 16:30), dan automatedSnapshotR etention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (a)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (a) kerahasia an dan integrita s informasi dan transaksi pelanggan dan rekanan	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
10.64 (a)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (a) kerahasia an dan integrita s informasi dan transaksi pelanggan dan rekanan	api-gw-cache-enabl ed-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (a)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (a) kerahasia an dan integrita s informasi dan transaksi pelanggan dan rekanan	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
10.64 (a)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (a) kerahasia an dan integrita s informasi dan transaksi pelanggan dan rekanan	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (a)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (a) kerahasia an dan integrita s informasi dan transaksi pelanggan dan rekanan	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomen dasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaa n enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.
10.64 (a)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (a) kerahasia an dan integrita s informasi dan transaksi pelanggan dan rekanan	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (a)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (a) kerahasia an dan integrita s informasi dan transaksi pelanggan dan rekanan	dynamodb-table-enc rypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindung i data tersebut. Secara default, tabel DynamoDB dienkrips i dengan kunci master pelanggan (CMK) AWS yang dimiliki.
10.64 (a)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (a) kerahasia an dan integrita s informasi dan transaksi pelanggan dan rekanan	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (a)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (a) kerahasia an dan integrita s informasi dan transaksi pelanggan dan rekanan	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
10.64 (a)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (a) kerahasia an dan integrita s informasi dan transaksi pelanggan dan rekanan	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (a)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (a) kerahasia an dan integrita s informasi dan transaksi pelanggan dan rekanan	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
10.64 (a)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (a) kerahasia an dan integrita s informasi dan transaksi pelanggan dan rekanan	opensearch-encrypt ed-at-rest	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk domain OpenSearc h Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (a)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (a) kerahasia an dan integrita s informasi dan transaksi pelanggan dan rekanan	opensearch-https-r equired	Karena data sensitif dapat ada dan membantu melindung i data dalam perjalana n, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
10.64 (a)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (a) kerahasia an dan integrita s informasi dan transaksi pelanggan dan rekanan	opensearch-node-to -node-pemeriksaan enkripsi-	Pastikan node-to-n ode enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkrip si memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (a)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (a) kerahasia an dan integrita s informasi dan transaksi pelanggan dan rekanan	rds-snapshot-encry pted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
10.64 (a)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (a) kerahasia an dan integrita s informasi dan transaksi pelanggan dan rekanan	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (a)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (a) kerahasia an dan integrita s informasi dan transaksi pelanggan dan rekanan	redshift-cluster-c onfiguration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastika n bahwa konfigura si yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberika n informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapka n untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (a)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (a) kerahasia an dan integrita s informasi dan transaksi pelanggan dan rekanan	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
10.64 (a)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (a) kerahasia an dan integrita s informasi dan transaksi pelanggan dan rekanan	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (a)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (a) kerahasia an dan integrita s informasi dan transaksi pelanggan dan rekanan	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
10.64 (a)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (a) kerahasia an dan integrita s informasi dan transaksi pelanggan dan rekanan	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (a)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (a) kerahasia an dan integrita s informasi dan transaksi pelanggan dan rekanan	sagemaker-endpoint -configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
10.64 (a)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (a) kerahasia an dan integrita s informasi dan transaksi pelanggan dan rekanan	sagemaker-notebook -instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (a)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (a) kerahasia an dan integrita s informasi dan transaksi pelanggan dan rekanan	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (a)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (a) kerahasia an dan integrita s informasi dan transaksi pelanggan dan rekanan	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (b)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (b) keandalan layanan yang disampaikan dari saluran dan perangkat dengan gangguan minimum terhadap layanan	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (b)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediak an layanan digital yang menjamin hal-hal berikut: (b) keandalan layanan yang disampaikan dari saluran dan perangkat dengan gangguan minimum terhadap layanan	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.
10.64 (b)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediak an layanan digital yang menjamin hal-hal berikut: (b) keandalan layanan yang disampaikan dari saluran dan perangkat dengan gangguan minimum terhadap layanan	elb-deletion-prote ction-enabled	Aturan ini memastika n bahwa Elastic Load Balancing memiliki perlindun gan penghapus an yang diaktifka n. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersedi aan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (b)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (b) keandalan layanan yang disampaikan dari saluran dan perangkat dengan gangguan minimum terhadap layanan	nlb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk NetworkLoad Balancer (NLBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (b)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (b) keandalan layanan yang disampaikan dari saluran dan perangkat dengan gangguan minimum terhadap layanan	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (b)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (b) keandalan layanan yang disampaikan dari saluran dan perangkat dengan gangguan minimum terhadap layanan	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) menyediakan ketersediaan dan daya tahan yang ditingkatkan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (b)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediak an layanan digital yang menjamin hal-hal berikut: (b) keandalan layanan yang disampaikan dari saluran dan perangkat dengan gangguan minimum terhadap layanan	rds-cluster-multi-az-diaktifkan	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) menyediakan ketersediaan dan daya tahan yang ditingkatkan untuk instans database. Saat Anda menyediak an instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastru ktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutk an operasi database

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			segera setelah failover selesai.
10.64 (b)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (b) keandalan layanan yang disampaikan dari saluran dan perangkat dengan gangguan minimum terhadap layanan	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (d)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (d) jejak audit yang memadai dan pemantauan transaksi anomali	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (d)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (d) jejak audit yang memadai dan pemantauan transaksi anomali	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (d)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (d) jejak audit yang memadai dan pemantauan transaksi anomali	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
10.64 (d)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (d) jejak audit yang memadai dan pemantauan transaksi anomali	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (d)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (d) jejak audit yang memadai dan pemantauan transaksi anomali	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (d)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (d) jejak audit yang memadai dan pemantauan transaksi anomali	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (d)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (d) jejak audit yang memadai dan pemantauan transaksi anomali	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
10.64 (d)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (d) jejak audit yang memadai dan pemantauan transaksi anomali	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (d)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (d) jejak audit yang memadai dan pemantauan transaksi anomali	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (d)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (d) jejak audit yang memadai dan pemantauan transaksi anomali	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (d)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (d) jejak audit yang memadai dan pemantauan transaksi anomali	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (d)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (d) jejak audit yang memadai dan pemantauan transaksi anomali	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (d)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (d) jejak audit yang memadai dan pemantauan transaksi anomali	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (d)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (d) jejak audit yang memadai dan pemantauan transaksi anomali	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (d)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (d) jejak audit yang memadai dan pemantauan transaksi anomali	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (d)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (d) jejak audit yang memadai dan pemantauan transaksi anomali	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (d)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (d) jejak audit yang memadai dan pemantauan transaksi anomali	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (d)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (d) jejak audit yang memadai dan pemantauan transaksi anomali	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (e)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (e) kemampuan untuk mengidentifikasi dan kembali ke titik pemulihan sebelum insiden atau gangguan layanan	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (e)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediak an layanan digital yang menjamin hal-hal berikut: (e) kemampuan untuk mengident ifikasi dan kembali ke titik pemulihan sebelum insiden atau gangguan layanan	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (e)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (e) kemampuan untuk mengidentifikasi dan kembali ke titik pemulihan sebelum insiden atau gangguan layanan	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (e)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (e) kemampuan untuk mengidentifikasi dan kembali ke titik pemulihan sebelum insiden atau gangguan layanan	dynamodb-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (e)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (e) kemampuan untuk mengidentifikasi dan kembali ke titik pemulihan sebelum insiden atau gangguan layanan	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (e)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (e) kemampuan untuk mengidentifikasi dan kembali ke titik pemulihan sebelum insiden atau gangguan layanan	ebs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (e)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (e) kemampuan untuk mengidentifikasi dan kembali ke titik pemulihan sebelum insiden atau gangguan layanan	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (e)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (e) kemampuan untuk mengidentifikasi dan kembali ke titik pemulihan sebelum insiden atau gangguan layanan	efs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (e)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediak an layanan digital yang menjamin hal-hal berikut: (e) kemampuan untuk mengident ifikasi dan kembali ke titik pemulihan sebelum insiden atau gangguan layanan	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (e)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (e) kemampuan untuk mengidentifikasi dan kembali ke titik pemulihan sebelum insiden atau gangguan layanan	rds-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Relational Database Service (Amazon RDS) Anda merupakan AWS bagian dari paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (e)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediakan layanan digital yang menjamin hal-hal berikut: (e) kemampuan untuk mengidentifikasi dan kembali ke titik pemulihan sebelum insiden atau gangguan layanan	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (e)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediak an layanan digital yang menjamin hal-hal berikut: (e) kemampuan untuk mengident ifikasi dan kembali ke titik pemulihan sebelum insiden atau gangguan layanan	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.64 (e)	Lembaga keuangan harus menerapkan kontrol keamanan teknologi yang kuat dalam menyediak an layanan digital yang menjamin hal-hal berikut: (e) kemampuan untuk mengident ifikasi dan kembali ke titik pemulihan sebelum insiden atau gangguan layanan	s3- -rencana resources-protected-by-backup	Untuk membantu proses pencadang an data, pastikan bucket Amazon Simple Storage Service (S3) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.7	Lembaga keuangan harus menggunak an alat yang efektif untuk mendukung pemantauan berkelanj utan dan proaktif serta deteksi tepat waktu aktivitas anomali dalam infrastruktur teknologinya. Ruang lingkup pemantaua n harus mencakup semua sistem kritis termasuk infrastruktur pendukung.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.7	Lembaga keuangan harus menggunak an alat yang efektif untuk mendukung pemantauan berkelanj utan dan proaktif serta deteksi tepat waktu aktivitas anomali dalam infrastruktur teknologinya. Ruang lingkup pemantaua n harus mencakup semua sistem kritis termasuk infrastruktur pendukung.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.8	Lembaga keuangan harus memastikan bahwa operasi keamanan sibernya terus mencegah dan mendeteksi potensi kompromi dari kontrol keamanannya atau melemahnya postur keamanannya. Untuk lembaga keuangan besar, ini harus mencakup melakukan penilaian kerentanan triwulanan komponen jaringan eksternal dan internal yang mendukung semua sistem kritis.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.8	Lembaga keuangan harus memastika n bahwa operasi keamanan sibernya terus mencegah dan mendeteksi potensi kompromi dari kontrol keamanannya atau melemahnya postur keamanannya. Untuk lembaga keuangan besar, ini harus mencakup melakukan penilaian kerentanan triwulanan komponen jaringan eksternal dan internal yang mendukung semua sistem kritis.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.18 (c) (f)	SOC harus dapat melakukan fungsi-fungsi berikut: (c) manajemen kerentana n; (f) penyediaan kesadaran situasion al untuk mendeteksi musuh dan ancaman termasuk analisis dan operasi intelijen ancaman, dan pemantauan indikator kompromi (IOC). Ini termasuk analisis perilaku tingkat lanjut untuk mendeteksi malware tanpa tanda tangan dan tanpa file dan untuk mengident ifikasi anomali yang dapat menimbulkan ancaman keamanan termasuk pada titik akhir dan lapisan jaringan.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.18 (c) (f)	SOC harus dapat melakukan fungsi-fungsi berikut: (c) manajemen kerentanan; (f) penyediaan kesadaran situasional untuk mendeteksi musuh dan ancaman termasuk analisis dan operasi intelijen ancaman, dan pemantauan indikator kompromi (IOC). Ini termasuk analisis perilaku tingkat lanjut untuk mendeteksi malware tanpa tanda tangan dan tanpa file dan untuk mengidentifikasi anomali yang dapat menimbulkan ancaman keamanan termasuk pada titik akhir dan lapisan jaringan.	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan: rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.18 (c) (f)	SOC harus dapat melakukan fungsi-fungsi berikut: (c) manajemen kerentana n; (f) penyediaan kesadaran situasion al untuk mendeteksi musuh dan ancaman termasuk analisis dan operasi intelijen ancaman, dan pemantauan indikator kompromi (IOC). Ini termasuk analisis perilaku tingkat lanjut untuk mendeteksi malware tanpa tanda tangan dan tanpa file dan untuk mengident ifikasi anomali yang dapat menimbulkan ancaman keamanan termasuk pada titik akhir dan lapisan jaringan.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 5.1	Melakukan tinjauan berkala pada pengaturan konfigura si dan aturan untuk semua perangkat keamanan. Gunakan alat otomatis untuk meninjau dan memantau perubahan pengaturan konfigura si dan aturan.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 5.1	Melakukan tinjauan berkala pada pengaturan konfigura si dan aturan untuk semua perangkat keamanan. Gunakan alat otomatis untuk meninjau dan memantau perubahan pengaturan konfigura si dan aturan.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 5.5 (b)	Pastikan kontrol keamanan untuk koneksi jaringan server-to-server eksternal meliputi: (b) penggunaan terowongan aman seperti Transport Layer Security (TLS) dan Virtual Private Network (VPN) IPSec	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Lampiran 5.5 (b)	Pastikan kontrol keamanan untuk koneksi jaringan server-to-server eksternal meliputi: (b) penggunaan terowongan aman seperti Transport Layer Security (TLS) dan Virtual Private Network (VPN) IPSec	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 5.5 (b)	Pastikan kontrol keamanan untuk koneksi jaringan server-to-server eksternal meliputi: (b) penggunaan terowongan aman seperti Transport Layer Security (TLS) dan Virtual Private Network (VPN) IPSec	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
Lampiran 5.5 (b)	Pastikan kontrol keamanan untuk koneksi jaringan server-to-server eksternal meliputi: (b) penggunaan terowongan aman seperti Transport Layer Security (TLS) dan Virtual Private Network (VPN) IPSec	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 5.5 (b)	Pastikan kontrol keamanan untuk koneksi jaringan server-to-server eksternal meliputi: (b) penggunaan terowongan aman seperti Transport Layer Security (TLS) dan Virtual Private Network (VPN) IPSec	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Lampiran 5.5 (b)	Pastikan kontrol keamanan untuk koneksi jaringan server-to-server eksternal meliputi: (b) penggunaan terowongan aman seperti Transport Layer Security (TLS) dan Virtual Private Network (VPN) IPSec	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 5.5 (c)	Pastikan kontrol keamanan untuk koneksi jaringan server-to-server eksternal meliputi: (c) menyebarkan server pementasan dengan pertahana n dan perlindun gan perimeter yang memadai seperti firewall, IPS, dan antivirus.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 5.5 (c)	Pastikan kontrol keamanan untuk koneksi jaringan server-to-server eksternal meliputi: (c) menyebarkan server pementasan dengan pertahana n dan perlindun gan perimeter yang memadai seperti firewall, IPS, dan antivirus.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 5.5 (c)	Pastikan kontrol keamanan untuk koneksi jaringan server-to-server eksternal meliputi: (c) menyebarkan server pementasan dengan pertahana n dan perlindun gan perimeter yang memadai seperti firewall, IPS, dan antivirus.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/ 0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 5.6	Pastikan kontrol keamanan untuk akses jarak jauh ke server mencakup hal-hal berikut: (a) membatasi akses hanya ke perangkat titik akhir yang diperkeras dan dikunci; (b) menggunakan terowongan aman seperti TLS dan VPN IPSec; (c) menyebarkan server 'gateway' dengan pertahanan dan perlindungan perimeter yang memadai seperti firewall, IPS dan antivirus; dan (d) menutup port yang relevan segera setelah kedaluwarsa akses jarak jauh.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 5.6	Pastikan kontrol keamanan untuk akses jarak jauh ke server mencakup hal-hal berikut: (a) membatasi akses hanya ke perangkat titik akhir yang diperkeras dan dikunci; (b) menggunakan terowongan aman seperti TLS dan VPN IPSec; (c) menyebark an server 'gateway' dengan pertahana n dan perlindun gan perimeter yang memadai seperti firewall, IPS dan antivirus; dan (d) menutup port yang relevan segera setelah kedaluwarsa akses jarak jauh.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 5.6	Pastikan kontrol keamanan untuk akses jarak jauh ke server mencakup hal-hal berikut: (a) membatasi akses hanya ke perangkat titik akhir yang diperkeras dan dikunci; (b) menggunakan terowongan aman seperti TLS dan VPN IPSec; (c) menyebarkan server 'gateway' dengan pertahanan dan perlindungan perimeter yang memadai seperti firewall, IPS dan antivirus; dan (d) menutup port yang relevan segera setelah kedaluwarsa akses jarak jauh.	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 5.6	Pastikan kontrol keamanan untuk akses jarak jauh ke server mencakup hal-hal berikut: (a) membatasi akses hanya ke perangkat titik akhir yang diperkeras dan dikunci; (b) menggunakan terowongan aman seperti TLS dan VPN IPSec; (c) menyebark an server 'gateway' dengan pertahana n dan perlindun gan perimeter yang memadai seperti firewall, IPS dan antivirus; dan (d) menutup port yang relevan segera setelah kedaluwarsa akses jarak jauh.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 5.6	Pastikan kontrol keamanan untuk akses jarak jauh ke server mencakup hal-hal berikut: (a) membatasi akses hanya ke perangkat titik akhir yang diperkeras dan dikunci; (b) menggunakan terowongan aman seperti TLS dan VPN IPSec; (c) menyebark an server 'gateway' dengan pertahana n dan perlindun gan perimeter yang memadai seperti firewall, IPS dan antivirus; dan (d) menutup port yang relevan segera setelah kedaluwarsa akses jarak jauh.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 5.6	Pastikan kontrol keamanan untuk akses jarak jauh ke server mencakup hal-hal berikut: (a) membatasi akses hanya ke perangkat titik akhir yang diperkeras dan dikunci; (b) menggunakan terowongan aman seperti TLS dan VPN IPSec; (c) menyebarkan server 'gateway' dengan pertahanan dan perlindungan perimeter yang memadai seperti firewall, IPS dan antivirus; dan (d) menutup port yang relevan segera setelah kedaluwarsa akses jarak jauh.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 1 (a)	Lembaga keuangan harus merancang arsitektur cloud yang kuat dan memastikan desain tersebut sesuai dengan standar internasional yang relevan untuk aplikasi yang dimaksud.	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.
Lampiran 10 Bagian B - 1 (b)	Sebuah lembaga keuangan didorong untuk mengadopsi prinsip-prinsip zero-trust untuk menyediakan arsitektur tangguh cyber dengan mengadopsi pola pikir “asumsi pelanggaran”, melapisi defense-in-depth melalui segmentasi mikro, ""“, hak akses deny-by-default “paling tidak istimewa”, dan melakukan inspeksi mendalam dan validasi berkelanjutan jika berlaku.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 1 (b)	Sebuah lembaga keuangan didorong untuk mengadopsi prinsip-prinsip zero-trust untuk menyediakan arsitektur tangguh cyber dengan mengadopsi pola pikir “asumsi pelanggaran”, melapisi defense-in-depth melalui segmentasi mikro, ""“, hak akses deny-by-default “paling tidak istimewa”, dan melakukan inspeksi mendalam dan validasi berkelanjutan jika berlaku.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 1 (b)	Sebuah lembaga keuangan didorong untuk mengadopsi prinsip-prinsip zero-trust untuk menyediakan arsitektur tangguh cyber dengan mengadopsi pola pikir “asumsi pelanggaran”, melapisi defense-in-depth melalui segmentasi mikro, ""“, hak akses deny-by-default “paling tidak istimewa”, dan melakukan inspeksi mendalam dan validasi berkelanjutan jika berlaku.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 1 (b)	Sebuah lembaga keuangan didorong untuk mengadopsi prinsip-prinsip zero-trust untuk menyediakan arsitektur tangguh cyber dengan mengadopsi pola pikir “asumsi pelanggaran”, melapisi defense-in-depth melalui segmentasi mikro, ""“, hak akses deny-by-default “paling tidak istimewa”, dan melakukan inspeksi mendalam dan validasi berkelanjutan jika berlaku.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 1 (c)	Lembaga keuangan harus menggunakan pendekatan arsitektur jaringan terbaru dan konsep dan solusi desain jaringan yang sesuai untuk mengelola dan memantau keamanan jaringan granular dan penyediaan jaringan terpusat dalam mengelola kompleksitas lingkungan jaringan cloud.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 1 (c)	Lembaga keuangan harus menggunakan pendekatan arsitektur jaringan terbaru dan konsep dan solusi desain jaringan yang sesuai untuk mengelola dan memantau keamanan jaringan granular dan penyediaan jaringan terpusat dalam mengelola kompleksitas lingkungan jaringan cloud.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
Lampiran 10 Bagian B - 1 (d)	Lembaga keuangan harus membangun dan memanfaatkan saluran komunikasi yang aman dan terenkripsi untuk memigrasikan server fisik, aplikasi, atau data ke platform cloud.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 1 (d)	Lembaga keuangan harus membangun dan memanfaatkan saluran komunikasi yang aman dan terenkripsi untuk memigrasikan server fisik, aplikasi, atau data ke platform cloud.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 1 (f) i)	Meningkatnya penggunaa n antarmuka pemrograman aplikasi (API) oleh lembaga keuangan untuk interkoneksi dengan penyedia layanan aplikasi eksternal dapat mencapai efisiensi dalam pemberian layanan baru. Namun, ini dapat meningkatkan permukaan serangan cyber dan kesalahan manajemen apa pun dapat memperkua t dampak insiden keamanan informasi . Lembaga keuangan harus memastika n bahwa APIs mereka tunduk pada mekanisme manajemen dan kontrol yang ketat yang meliputi hal-hal berikut: i) APIs harus dirancang untuk ketahanan layanan untuk menghinda ri risiko satu titik kegagalan dan	api-gwv2- authoriza tion-type-configured	Pastikan rute API Amazon API Gateway v2 Anda memiliki jenis otorisasi yang disetel untuk mencegah akses tidak sah ke sumber daya backend yang mendasarinya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dikonfigurasi secara aman dengan kontrol akses yang tepat;		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 1 (f) ii)	Meningkatnya penggunaa n antarmuka pemrograman aplikasi (API) oleh lembaga keuangan untuk interkoneksi dengan penyedia layanan aplikasi eksternal dapat mencapai efisiensi dalam pemberian layanan baru. Namun, ini dapat meningkatkan permukaan serangan cyber dan kesalahan manajemen apa pun dapat memperkua t dampak insiden keamanan informasi . Lembaga keuangan harus memastika n bahwa APIs mereka tunduk pada mekanisme manajemen dan kontrol yang ketat yang meliputi hal-hal berikut: ii) APIs harus dilacak dan dipantau terhadap serangan cyber dengan langkah-langkah respons insiden yang	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizink an, memblokir, atau menghitung permintaa n web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindung inya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memadai dan tidak ditugaskan secara tepat waktu ketika tidak lagi digunakan.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 1 (f) ii)	Meningkatnya penggunaa n antarmuka pemrograman aplikasi (API) oleh lembaga keuangan untuk interkoneksi dengan penyedia layanan aplikasi eksternal dapat mencapai efisiensi dalam pemberian layanan baru. Namun, ini dapat meningkatkan permukaan serangan cyber dan kesalahan manajemen apa pun dapat memperkua t dampak insiden keamanan informasi . Lembaga keuangan harus memastika n bahwa APIs mereka tunduk pada mekanisme manajemen dan kontrol yang ketat yang meliputi hal-hal berikut: ii) APIs harus dilacak dan dipantau terhadap serangan cyber dengan langkah-langkah respons insiden yang	api-gw-execution-l ogging-diaktifkan	Pencatatan API Gateway menampilk an tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memadai dan tidak ditugaskan secara tepat waktu ketika tidak lagi digunakan.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 2 (b) ii)	Lembaga keuangan harus terus memanfaatkan kemampuan cloud yang ditingkatkan untuk meningkatkan keamanan layanan cloud dan lembaga keuangan, antara lain, didorong untuk: ii) menggunakan praktik infrastru ktur yang tidak dapat diubah untuk penyebaran layanan untuk mengurang i risiko kegagalan dengan menciptak an lingkungan baru dengan versi stabil terbaru dari perangkat lunak. Pemantauan lingkungan cloud yang sedang berlangsu ng harus mencakup otomatisasi deteksi perubahan pada infrastruktur yang tidak dapat diubah untuk meningkatkan tinjauan kepatuhan dan memerangi serangan cyber yang berkembang	cloudformation-stack-notification-check	Untuk mendeteks i perubahan yang tidak diinginkan pada AWS sumber daya yang mendasarinya, pastikan CloudForm ation tumpukan Anda dikonfigurasi untuk mengirim pemberita huan peristiwa ke topik Amazon SNS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 3 (b) vi)	Lembaga keuangan harus memastikan mesin virtual dan gambar kontainer dikonfigurasi, dikeraskan, dan dipantau dengan tepat. Ini termasuk yang berikut: vi) gambar yang disimpan dikenakan pemantauan keamanan dari akses dan perubahan yang tidak sah.	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 5 (a) i)	Sebagai bagian dari kemampuan pemulihan yang efektif, lembaga keuangan harus memastikan prosedur pencadangan dan pemulihan yang ada diperluas untuk mencakup layanan cloud, yang meliputi: i) mendefinisikan dan memformalkan strategi pencadangan dan pemulihan pada tahap perencanaan adopsi cloud;	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 5 (a) i)	Sebagai bagian dari kemampuan pemulihan yang efektif, lembaga keuangan harus memastikan prosedur pencadangan dan pemulihan yang ada diperluas untuk mencakup layanan cloud, yang meliputi: i) mendefinisikan dan memformalkan strategi pencadangan dan pemulihan pada tahap perencanaan adopsi cloud;	dynamodb-resources-protected-by-rencana cadangan	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 5 (a) i)	Sebagai bagian dari kemampuan pemulihan yang efektif, lembaga keuangan harus memastikan prosedur pencadangan dan pemulihan yang ada diperluas untuk mencakup layanan cloud, yang meliputi: i) mendefinisikan dan memformalkan strategi pencadangan dan pemulihan pada tahap perencanaan adopsi cloud;	ebs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 5 (a) i)	Sebagai bagian dari kemampuan pemulihan yang efektif, lembaga keuangan harus memastikan prosedur pencadangan dan pemulihan yang ada diperluas untuk mencakup layanan cloud, yang meliputi: i) mendefinisikan dan memformalkan strategi pencadangan dan pemulihan pada tahap perencanaan adopsi cloud;	efs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 5 (a) i)	Sebagai bagian dari kemampuan pemulihan yang efektif, lembaga keuangan harus memastikan prosedur pencadangan dan pemulihan yang ada diperluas untuk mencakup layanan cloud, yang meliputi: i) mendefinisikan dan memformalkan strategi pencadangan dan pemulihan pada tahap perencanaan adopsi cloud;	rds-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Relational Database Service (Amazon RDS) Anda merupakan AWS bagian dari paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 5 (a) i)	Sebagai bagian dari kemampuan pemulihan yang efektif, lembaga keuangan harus memastikan prosedur pencadangan dan pemulihan yang ada diperluas untuk mencakup layanan cloud, yang meliputi: i) mendefinisikan dan memformalkan strategi pencadangan dan pemulihan pada tahap perencanaan adopsi cloud;	s3- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan bucket Amazon Simple Storage Service (S3) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 5 (b)	Lembaga keuangan harus memastikan prosedur pencadangan dan restorasi diuji secara berkala untuk memvalidasi kemampuan pemulihan. Frekuensi prosedur pencadangan harus sepadan dengan kekritisan sistem dan tujuan titik pemulihan (RPO) sistem. Tindakan perbaikan harus segera diambil oleh lembaga keuangan untuk pencadangan yang gagal.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 5 (c) i)	Lembaga keuangan harus memastikan pencadangan dan pemulihan mesin virtual dan wadah yang memadai termasuk pengaturan konfigurasi cadangan (untuk IaaS dan PaaS, jika relevan), yang meliputi: i) memastikan kemampuan untuk memulihkan mesin virtual dan wadah pada point-in-time sebagaimana ditentukan oleh tujuan pemulihan bisnis;	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 5 (d) i)	Lembaga keuangan harus menilai persyaratan ketahanan layanan cloud dan mengident ifikasi langkah-l angkah yang tepat yang sepadan dengan kekritisan sistem, untuk memastikan ketersediaan layanan dalam skenario yang sangat merugikan. Lembaga keuangan harus mempertim bangkan pendekata n berbasis risiko dan secara progresif mengadopsi kontrol mitigasi yang tepat untuk memastikan ketersediaan layanan dan mengurang i risiko konsentra si. Di antara opsi yang layak adalah: i) memanfaatkan ketersediaan tinggi dan fitur redundansi layanan cloud untuk memastikan pusat data produksi memiliki kapasitas redundan	autoscaling-multiple-az	Untuk memastika n ketersediaan tinggi, pastikan grup Auto Scaling Anda dikonfigurasi untuk menjangkau beberapa Availability Zone.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	di zona ketersediaan yang berbeda;		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 5 (d) i)	Lembaga keuangan harus menilai persyaratan ketahanan layanan cloud dan mengident ifikasi langkah-l angkah yang tepat yang sepadan dengan kekritisan sistem, untuk memastikan ketersediaan layanan dalam skenario yang sangat merugikan. Lembaga keuangan harus mempertim bangkan pendekata n berbasis risiko dan secara progresif mengadopsi kontrol mitigasi yang tepat untuk memastikan ketersediaan layanan dan mengurang i risiko konsentra si. Di antara opsi yang layak adalah: i) memanfaatkan ketersediaan tinggi dan fitur redundansi layanan cloud untuk memastikan pusat data produksi memiliki kapasitas redundan	elbv2-multiple-az	Elastic Load Balancing (ELB) secara otomatis mendistribusikan lalu lintas masuk Anda di beberapa target, seperti EC2 instance, kontainer, dan alamat IP, di zona ketersedi aan. Untuk memastika n ketersediaan tinggi, pastikan ELB Anda telah mendaftarkan instans dari beberapa Availability Zone.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	di zona ketersediaan yang berbeda;		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 5 (d) i)	Lembaga keuangan harus menilai persyaratan ketahanan layanan cloud dan mengident ifikasi langkah-l angkah yang tepat yang sepadan dengan kekritisan sistem, untuk memastikan ketersediaan layanan dalam skenario yang sangat merugikan. Lembaga keuangan harus mempertim bangkan pendekata n berbasis risiko dan secara progresif mengadopsi kontrol mitigasi yang tepat untuk memastikan ketersediaan layanan dan mengurang i risiko konsentra si. Di antara opsi yang layak adalah: i) memanfaatkan ketersediaan tinggi dan fitur redundansi layanan cloud untuk memastikan pusat data produksi memiliki kapasitas redundan	lambda-vpc-multi-az-periksa	Jika fungsi AWS Lambda Anda dikonfigurasi untuk terhubung ke virtual private cloud (VPC) di akun Anda, gunakan fungsi AWS Lambda di setidaknya dua Availability Zone yang berbeda untuk memastikan bahwa fungsi Anda tersedia untuk memproses peristiwa jika terjadi gangguan layanan di satu zona.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	di zona ketersediaan yang berbeda;		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 5 (d) i)	Lembaga keuangan harus menilai persyaratan ketahanan layanan cloud dan mengident ifikasi langkah-l angkah yang tepat yang sepadan dengan kekritisan sistem, untuk memastikan ketersediaan layanan dalam skenario yang sangat merugikan. Lembaga keuangan harus mempertim bangkan pendekata n berbasis risiko dan secara progresif mengadopsi kontrol mitigasi yang tepat untuk memastikan ketersediaan layanan dan mengurang i risiko konsentra si. Di antara opsi yang layak adalah: i) memanfaatkan ketersediaan tinggi dan fitur redundansi layanan cloud untuk memastikan pusat data produksi memiliki kapasitas redundan	nlb-cross-zone-loa d-menyeimbangkan diaktifkan	Aktifkan penyeimba ngan beban lintas zona untuk NetworkLo ad Balancer (NLBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimba ngan beban lintas zona mengurang i kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkat kan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	di zona ketersediaan yang berbeda;		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 5 (d) i)	Lembaga keuangan harus menilai persyaratan ketahanan layanan cloud dan mengident ifikasi langkah-l angkah yang tepat yang sepadan dengan kekritisan sistem, untuk memastikan ketersediaan layanan dalam skenario yang sangat merugikan. Lembaga keuangan harus mempertim bangkan pendekata n berbasis risiko dan secara progresif mengadopsi kontrol mitigasi yang tepat untuk memastikan ketersediaan layanan dan mengurang i risiko konsentra si. Di antara opsi yang layak adalah: i) memanfaatkan ketersediaan tinggi dan fitur redundansi layanan cloud untuk memastikan pusat data produksi memiliki kapasitas redundan	rds-cluster-multi-az-diaktifkan	Cluster Amazon Relational Database Service (Amazon RDS) harus mengaktif kan replikasi Multi-AZ untuk membantu ketersediaan data yang disimpan. Setiap Availability Zone berjalan pada infrastru ktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutk an operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	di zona ketersediaan yang berbeda;		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 5 (d) i)	Lembaga keuangan harus menilai persyaratan ketahanan layanan cloud dan mengident ifikasi langkah-l angkah yang tepat yang sepadan dengan kekritisan sistem, untuk memastikan ketersediaan layanan dalam skenario yang sangat merugikan. Lembaga keuangan harus mempertim bangkan pendekata n berbasis risiko dan secara progresif mengadopsi kontrol mitigasi yang tepat untuk memastikan ketersediaan layanan dan mengurang i risiko konsentra si. Di antara opsi yang layak adalah: i) memanfaatkan ketersediaan tinggi dan fitur redundansi layanan cloud untuk memastikan pusat data produksi memiliki kapasitas redundan	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) menyediakan ketersediaan dan daya tahan yang ditingkatkan untuk instans database. Saat Anda menyediak an instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastru ktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutk an operasi database

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	di zona ketersediaan yang berbeda;		segera setelah failover selesai.
Lampiran 10 Bagian B - 8 (a)	Lembaga keuangan harus menerapkan teknik enkripsi yang tepat dan relevan untuk melindung i kerahasiaan dan integritas data sensitif yang disimpan di cloud.	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Lampiran 10 Bagian B - 8 (a)	Lembaga keuangan harus menerapkan teknik enkripsi yang tepat dan relevan untuk melindung i kerahasiaan dan integritas data sensitif yang disimpan di cloud.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 8 (a)	Lembaga keuangan harus menerapkan teknik enkripsi yang tepat dan relevan untuk melindung i kerahasiaan dan integritas data sensitif yang disimpan di cloud.	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomen dasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaa n enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.
Lampiran 10 Bagian B - 8 (a)	Lembaga keuangan harus menerapkan teknik enkripsi yang tepat dan relevan untuk melindung i kerahasiaan dan integritas data sensitif yang disimpan di cloud.	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 8 (a)	Lembaga keuangan harus menerapkan teknik enkripsi yang tepat dan relevan untuk melindung i kerahasiaan dan integritas data sensitif yang disimpan di cloud.	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindung i data tersebut. Secara default, tabel DynamoDB dienkrips i dengan kunci master pelanggan (CMK) AWS yang dimiliki.
Lampiran 10 Bagian B - 8 (a)	Lembaga keuangan harus menerapkan teknik enkripsi yang tepat dan relevan untuk melindung i kerahasiaan dan integritas data sensitif yang disimpan di cloud.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 8 (a)	Lembaga keuangan harus menerapkan teknik enkripsi yang tepat dan relevan untuk melindung i kerahasiaan dan integritas data sensitif yang disimpan di cloud.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
Lampiran 10 Bagian B - 8 (a)	Lembaga keuangan harus menerapkan teknik enkripsi yang tepat dan relevan untuk melindung i kerahasiaan dan integritas data sensitif yang disimpan di cloud.	eks-secrets-encrypted	Untuk membantu melindungi data saat istirahat, pastikan klaster Amazon Elastic Kubernetes Service (EKS) Anda dikonfigurasi agar rahasia Kubernete s dienkripsi. Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 8 (a)	Lembaga keuangan harus menerapkan teknik enkripsi yang tepat dan relevan untuk melindung i kerahasiaan dan integritas data sensitif yang disimpan di cloud.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
Lampiran 10 Bagian B - 8 (a)	Lembaga keuangan harus menerapkan teknik enkripsi yang tepat dan relevan untuk melindung i kerahasiaan dan integritas data sensitif yang disimpan di cloud.	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk domain OpenSearc h Layanan Amazon Anda.
Lampiran 10 Bagian B - 8 (a)	Lembaga keuangan harus menerapkan teknik enkripsi yang tepat dan relevan untuk melindung i kerahasiaan dan integritas data sensitif yang disimpan di cloud.	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 8 (a)	Lembaga keuangan harus menerapkan teknik enkripsi yang tepat dan relevan untuk melindung i kerahasiaan dan integritas data sensitif yang disimpan di cloud.	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Lampiran 10 Bagian B - 8 (a)	Lembaga keuangan harus menerapkan teknik enkripsi yang tepat dan relevan untuk melindung i kerahasiaan dan integritas data sensitif yang disimpan di cloud.	s3- default-encryption -kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 8 (a)	Lembaga keuangan harus menerapkan teknik enkripsi yang tepat dan relevan untuk melindung i kerahasiaan dan integritas data sensitif yang disimpan di cloud.	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 8 (a)	Lembaga keuangan harus menerapkan teknik enkripsi yang tepat dan relevan untuk melindung i kerahasiaan dan integritas data sensitif yang disimpan di cloud.	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 8 (d)	Ketika penggunaan adopsi cloud meningkat, mengelola banyak kunci enkripsi yang digunakan untuk melindungi data menjadi lebih kompleks dan dapat menimbulkan tantangan baru bagi lembaga keuangan. Lembaga keuangan harus mengadopsi pendekatan yang komprehensif dan terpusat untuk manajemen kunci termasuk penggunaan sistem manajemen kunci terpusat yang dapat menangani generasi, penyimpanan dan distribusi kunci dengan cara yang aman dan terukur.	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 8 (d)	Ketika penggunaan adopsi cloud meningkat, mengelola banyak kunci enkripsi yang digunakan untuk melindungi data menjadi lebih kompleks dan dapat menimbulkan tantangan baru bagi lembaga keuangan. Lembaga keuangan harus mengadopsi pendekatan yang komprehensif dan terpusat untuk manajemen kunci termasuk penggunaan sistem manajemen kunci terpusat yang dapat menangani generasi, penyimpanan dan distribusi kunci dengan cara yang aman dan terukur.	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 9 (a) ii)	Bidang manajemen adalah perbedaan keamanan utama antara infrastru ktur tradisional dan komputasi awan di mana akses jarak jauh didukung secara default. Lapisan akses ini bisa rentan terhadap serangan cyber sehingga membahayakan integritas seluruh penyebaran cloud. Mengingat hal ini, Lembaga keuangan harus memastikan penggunaan kontrol yang kuat untuk mengakses bidang manajemen yang dapat mencakup hal-hal berikut: ii) menerapkan “hak istimewa paling kecil” dan otentikasi multi-faktor yang kuat (MFA) misalnya, kata sandi yang kuat, token lunak, alat manajemen akses istimewa dan fungsi pemeriksa pembuat;	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifik asi berdasark an kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkin kan Anda untuk mengatur secara opsional RequireUp percaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 9 (a) ii)	Bidang manajemen adalah perbedaan keamanan utama antara infrastru ktur tradisional dan komputasi awan di mana akses jarak jauh didukung secara default. Lapisan akses ini bisa rentan terhadap serangan cyber sehingga membahayakan integritas seluruh penyebaran cloud. Mengingat hal ini, Lembaga keuangan harus memastikan penggunaan kontrol yang kuat untuk mengakses bidang manajemen yang dapat mencakup hal-hal berikut: ii) menerapkan “hak istimewa paling kecil” dan otentikasi multi-faktor yang kuat (MFA) misalnya, kata sandi yang kuat, token lunak, alat manajemen akses istimewa dan fungsi pemeriksa pembuat;	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastika n otentikasi multi-fak tor (MFA) diaktifka n untuk semua pengguna IAM. MFA menambahk an lapisan perlindun gan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna IAM.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 9 (a) ii)	Bidang manajemen adalah perbedaan keamanan utama antara infrastru ktur tradisional dan komputasi awan di mana akses jarak jauh didukung secara default. Lapisan akses ini bisa rentan terhadap serangan cyber sehingga membahayakan integritas seluruh penyebaran cloud. Mengingat hal ini, Lembaga keuangan harus memastikan penggunaan kontrol yang kuat untuk mengakses bidang manajemen yang dapat mencakup hal-hal berikut: ii) menerapkan “hak istimewa paling kecil” dan otentikasi multi-faktor yang kuat (MFA) misalnya, kata sandi yang kuat, token lunak, alat manajemen akses istimewa dan fungsi pemeriksa pembuat;	root-account-hardw are-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindun gan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 9 (a) ii)	Bidang manajemen adalah perbedaan keamanan utama antara infrastru ktur tradisional dan komputasi awan di mana akses jarak jauh didukung secara default. Lapisan akses ini bisa rentan terhadap serangan cyber sehingga membahayakan integritas seluruh penyebaran cloud. Mengingat hal ini, Lembaga keuangan harus memastikan penggunaan kontrol yang kuat untuk mengakses bidang manajemen yang dapat mencakup hal-hal berikut: ii) menerapkan “hak istimewa paling kecil” dan otentikasi multi-faktor yang kuat (MFA) misalnya, kata sandi yang kuat, token lunak, alat manajemen akses istimewa dan fungsi pemeriksa pembuat;	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindun gan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 9 (a) iii)	Bidang manajemen adalah perbedaan keamanan utama antara infrastru ktur tradisional dan komputasi awan di mana akses jarak jauh didukung secara default. Lapisan akses ini bisa rentan terhadap serangan cyber sehingga membahayakan integritas seluruh penyebaran cloud. Dalam pandangan ini, Lembaga keuangan harus memastikan penggunaan kontrol yang kuat untuk mengakses bidang manajemen yang dapat mencakup hal-hal berikut: iii) menggunakan alokasi hak granular untuk pengguna istimewa;	iam-policy-no-statements-with-admin-access	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 9 (a) iii)	Bidang manajemen adalah perbedaan keamanan utama antara infrastru ktur tradisional dan komputasi awan di mana akses jarak jauh didukung secara default. Lapisan akses ini bisa rentan terhadap serangan cyber sehingga membahayakan integritas seluruh penyebaran cloud. Dalam pandangan ini, Lembaga keuangan harus memastikan penggunaan kontrol yang kuat untuk mengakses bidang manajemen yang dapat mencakup hal-hal berikut: iii) menggunakan alokasi hak granular untuk pengguna istimewa;	iam-user-no-policies-periksa	Aturan ini memastika n kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapka n hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 9 (a) iv)	Bidang manajemen adalah perbedaan keamanan utama antara infrastru ktur tradisional dan komputasi awan di mana akses jarak jauh didukung secara default. Lapisan akses ini bisa rentan terhadap serangan cyber sehingga membahayakan integritas seluruh penyebaran cloud. Dalam pandangan ini, Lembaga keuangan harus memastikan penggunaan kontrol yang kuat untuk mengakses bidang manajemen yang dapat mencakup hal-hal berikut: iv) melakukan pemantauan terus menerus terhadap kegiatan yang dilakukan oleh pengguna istimewa;	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomen dasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaa n enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 9 (a) iv)	Bidang manajemen adalah perbedaan keamanan utama antara infrastru ktur tradisional dan komputasi awan di mana akses jarak jauh didukung secara default. Lapisan akses ini bisa rentan terhadap serangan cyber sehingga membahayakan integritas seluruh penyebaran cloud. Dalam pandangan ini, Lembaga keuangan harus memastikan penggunaan kontrol yang kuat untuk mengakses bidang manajemen yang dapat mencakup hal-hal berikut: iv) melakukan pemantauan terus menerus terhadap kegiatan yang dilakukan oleh pengguna istimewa;	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 12 (a)	Lembaga keuangan harus melindungi data yang dihosting di layanan cloud sebagaimana disyaratkan di bawah bagian Pencegaha n Kehilangan Data (paragraf 11.14 hingga 11.16) dari dokumen kebijakan ini, termasuk perluasan jejak titik akhir jika lembaga keuangan mengizinkan stafnya menggunakan perangkat mereka sendiri untuk mengakses data sensitif.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 12 (a)	Lembaga keuangan harus melindungi data yang dihosting di layanan cloud sebagaimana disyaratkan di bawah bagian Pencegaha n Kehilangan Data (paragraf 11.14 hingga 11.16) dari dokumen kebijakan ini, termasuk perluasan jejak titik akhir jika lembaga keuangan mengizinkan stafnya menggunakan perangkat mereka sendiri untuk mengakses data sensitif.	macie-status-check	Amazon Macie adalah layanan keamanan data yang menggunakan machine learning (ML) dan pencocokan pola untuk menemukan dan membantu melindungi data sensitif Anda yang tersimpan di bucket Amazon Simple Storage Service (S3).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 14 (c) i)	Lembaga keuangan harus mempertim bangkan langkah-l angkah tambahan berikut dalam pengembangan CIRP-nya: i) meningkat kan kemampuannya untuk mendeteksi insiden pelanggar an keamanan untuk mencapai manajemen insiden yang efektif, termasuk kemampuan untuk mendeteksi kebocoran data di web gelap;	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lampiran 10 Bagian B - 14 (c) i)	Lembaga keuangan harus mempertim bangkan langkah-l angkah tambahan berikut dalam pengembangan CIRP-nya: i) meningkat kan kemampuannya untuk mendeteksi insiden pelanggar an keamanan untuk mencapai manajemen insiden yang efektif, termasuk kemampuan untuk mendeteksi kebocoran data di web gelap;	guardduty-non-arch ived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasark an tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunak an klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSe v (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratk an oleh kebijakan organisasi Anda.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk BNM RMi T.

Praktik Terbaik Operasional untuk Profil Kontrol Cloud Sedang Pusat Keamanan Siber Kanada (CCCS)

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara Canadian Centre for Cyber Security (CCCS) Medium Cloud Control Profile dan aturan AWS Config terkelola. Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau beberapa kontrol CCCS Medium Cloud Control Profile. Kontrol Profil Kontrol Cloud Medium CCCS dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCC-FPBMM-AC-2 (1)	AC-2 (1) Manajemen Akun | Manajemen Akun Sistem Otomatis	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			terlihat dalam Isi AWS CloudTrail Rekam.
CCC-FPBMM-AC-2 (1)	AC-2 (1) Manajemen Akun | Manajemen Akun Sistem Otomatis	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCC-FPBMM-AC-2 (1)	AC-2 (1) Manajemen Akun | Manajemen Akun Sistem Otomatis	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCC-FPBMM-AC-2 (1)	AC-2 (1) Manajemen Akun | Manajemen Akun Sistem Otomatis	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCC-FPBMM-AC-2 (1)	AC-2 (1) Manajemen Akun | Manajemen Akun Sistem Otomatis	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
CCC-FPBMM-AC-2 (1)	AC-2 (1) Manajemen Akun | Manajemen Akun Sistem Otomatis	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCC-FPBMM-AC-2 (1)	AC-2 (1) Manajemen Akun | Manajemen Akun Sistem Otomatis	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
CCC-FPBMM-AC-2 (1)	AC-2 (1) Manajemen Akun | Manajemen Akun Sistem Otomatis	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCC-FPBMM-AC-2 (1)	AC-2 (1) Manajemen Akun | Manajemen Akun Sistem Otomatis	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCC-FPBMM-AC-2 (1)	AC-2 (1) Manajemen Akun | Manajemen Akun Sistem Otomatis	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
CCC-FPBMM-AC-2 (1)	AC-2 (1) Manajemen Akun | Manajemen Akun Sistem Otomatis	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCC-FPBMM-AC-2 (1)	AC-2 (1) Manajemen Akun | Manajemen Akun Sistem Otomatis	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCC-FPBMM-AC-2 (1)	AC-2 (1) Manajemen Akun | Manajemen Akun Sistem Otomatis	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCC-FPBMM-AC-2 (1)	AC-2 (1) Manajemen Akun | Manajemen Akun Sistem Otomatis	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensi yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCC-FPBMM-AC-2 (1)	AC-2 (1) Manajemen Akun | Manajemen Akun Sistem Otomatis	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2 (3)	AC-2 (3) Manajemen Akun | Nonaktifkan Akun Tidak Aktif	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2 (3)	AC-2 (3) Manajemen Akun | Nonaktifkan Akun Tidak Aktif	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensi yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2 (4)	AC-2 (4) Manajemen Akun | Tindakan Audit Otomatis	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
CCCS-FPBMM-AC-2 (4)	AC-2 (4) Manajemen Akun | Tindakan Audit Otomatis	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2 (4)	AC-2 (4) Manajemen Akun | Tindakan Audit Otomatis	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2 (4)	AC-2 (4) Manajemen Akun | Tindakan Audit Otomatis	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2 (4)	AC-2 (4) Manajemen Akun | Tindakan Audit Otomatis	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2 (4)	AC-2 (4) Manajemen Akun | Tindakan Audit Otomatis	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2 (4)	AC-2 (4) Manajemen Akun | Tindakan Audit Otomatis	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.A	AC-2.A Manajemen Akun	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.A	AC-2.A Manajemen Akun	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.A	AC-2.A Manajemen Akun	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.A	AC-2.A Manajemen Akun	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.A	AC-2.A Manajemen Akun	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
CCCS-FPBMM-AC-2.A	AC-2.A Manajemen Akun	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.A	AC-2.A Manajemen Akun	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-AC-2.A	AC-2.A Manajemen Akun	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.A	AC-2.A Manajemen Akun	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.A	AC-2.A Manajemen Akun	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
CCCS-FPBMM-AC-2.A	AC-2.A Manajemen Akun	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.A	AC-2.A Manajemen Akun	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.A	AC-2.A Manajemen Akun	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.A	AC-2.A Manajemen Akun	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensi yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.A	AC-2.A Manajemen Akun	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.b	AC-2.B Manajemen Akun	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.b	AC-2.B Manajemen Akun	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.b	AC-2.B Manajemen Akun	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.b	AC-2.B Manajemen Akun	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.b	AC-2.B Manajemen Akun	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
CCCS-FPBMM-AC-2.b	AC-2.B Manajemen Akun	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.b	AC-2.B Manajemen Akun	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-AC-2.b	AC-2.B Manajemen Akun	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.b	AC-2.B Manajemen Akun	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.b	AC-2.B Manajemen Akun	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
CCCS-FPBMM-AC-2.b	AC-2.B Manajemen Akun	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.b	AC-2.B Manajemen Akun	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.b	AC-2.B Manajemen Akun	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.b	AC-2.B Manajemen Akun	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensi yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.b	AC-2.B Manajemen Akun	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.c	AC-2.C Manajemen Akun	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.c	AC-2.C Manajemen Akun	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.c	AC-2.C Manajemen Akun	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.c	AC-2.C Manajemen Akun	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.c	AC-2.C Manajemen Akun	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
CCCS-FPBMM-AC-2.c	AC-2.C Manajemen Akun	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.c	AC-2.C Manajemen Akun	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-AC-2.c	AC-2.C Manajemen Akun	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.c	AC-2.C Manajemen Akun	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.c	AC-2.C Manajemen Akun	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
CCCS-FPBMM-AC-2.c	AC-2.C Manajemen Akun	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.c	AC-2.C Manajemen Akun	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.c	AC-2.C Manajemen Akun	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.c	AC-2.C Manajemen Akun	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensi yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.c	AC-2.C Manajemen Akun	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.D	AC-2.D Manajemen Akun	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.D	AC-2.D Manajemen Akun	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.D	AC-2.D Manajemen Akun	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.D	AC-2.D Manajemen Akun	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.D	AC-2.D Manajemen Akun	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
CCCS-FPBMM-AC-2.D	AC-2.D Manajemen Akun	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.D	AC-2.D Manajemen Akun	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-AC-2.D	AC-2.D Manajemen Akun	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.D	AC-2.D Manajemen Akun	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.D	AC-2.D Manajemen Akun	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
CCCS-FPBMM-AC-2.D	AC-2.D Manajemen Akun	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.D	AC-2.D Manajemen Akun	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.D	AC-2.D Manajemen Akun	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.D	AC-2.D Manajemen Akun	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensi yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.D	AC-2.D Manajemen Akun	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.e	AC-2.E Manajemen Akun	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.e	AC-2.E Manajemen Akun	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.e	AC-2.E Manajemen Akun	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.e	AC-2.E Manajemen Akun	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.e	AC-2.E Manajemen Akun	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
CCCS-FPBMM-AC-2.e	AC-2.E Manajemen Akun	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.e	AC-2.E Manajemen Akun	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-AC-2.e	AC-2.E Manajemen Akun	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.e	AC-2.E Manajemen Akun	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.e	AC-2.E Manajemen Akun	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
CCCS-FPBMM-AC-2.e	AC-2.E Manajemen Akun	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.e	AC-2.E Manajemen Akun	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.e	AC-2.E Manajemen Akun	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.e	AC-2.E Manajemen Akun	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensi yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.e	AC-2.E Manajemen Akun	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.f	AC-2.F Manajemen Akun	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.f	AC-2.F Manajemen Akun	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.f	AC-2.F Manajemen Akun	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.f	AC-2.F Manajemen Akun	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.f	AC-2.F Manajemen Akun	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
CCCS-FPBMM-AC-2.f	AC-2.F Manajemen Akun	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.f	AC-2.F Manajemen Akun	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-AC-2.f	AC-2.F Manajemen Akun	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.f	AC-2.F Manajemen Akun	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.f	AC-2.F Manajemen Akun	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
CCCS-FPBMM-AC-2.f	AC-2.F Manajemen Akun	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.f	AC-2.F Manajemen Akun	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.f	AC-2.F Manajemen Akun	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.f	AC-2.F Manajemen Akun	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensi yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.f	AC-2.F Manajemen Akun	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.g	AC-2.G Manajemen Akun	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.g	AC-2.G Manajemen Akun	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.g	AC-2.G Manajemen Akun	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.g	AC-2.G Manajemen Akun	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.g	AC-2.G Manajemen Akun	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
CCCS-FPBMM-AC-2.g	AC-2.G Manajemen Akun	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.g	AC-2.G Manajemen Akun	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-AC-2.g	AC-2.G Manajemen Akun	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.g	AC-2.G Manajemen Akun	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.g	AC-2.G Manajemen Akun	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
CCCS-FPBMM-AC-2.g	AC-2.G Manajemen Akun	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.g	AC-2.G Manajemen Akun	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.g	AC-2.G Manajemen Akun	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.g	AC-2.G Manajemen Akun	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensi yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.g	AC-2.G Manajemen Akun	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.h	AC-2.H Manajemen Akun	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.h	AC-2.H Manajemen Akun	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.h	AC-2.H Manajemen Akun	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.h	AC-2.H Manajemen Akun	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.h	AC-2.H Manajemen Akun	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
CCCS-FPBMM-AC-2.h	AC-2.H Manajemen Akun	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.h	AC-2.H Manajemen Akun	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-AC-2.h	AC-2.H Manajemen Akun	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.h	AC-2.H Manajemen Akun	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.h	AC-2.H Manajemen Akun	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
CCCS-FPBMM-AC-2.h	AC-2.H Manajemen Akun	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.h	AC-2.H Manajemen Akun	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.h	AC-2.H Manajemen Akun	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.h	AC-2.H Manajemen Akun	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensi yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.h	AC-2.H Manajemen Akun	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.i	AC-2.I Manajemen Akun	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.i	AC-2.I Manajemen Akun	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.i	AC-2.I Manajemen Akun	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.i	AC-2.I Manajemen Akun	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.i	AC-2.I Manajemen Akun	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
CCCS-FPBMM-AC-2.i	AC-2.I Manajemen Akun	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.i	AC-2.I Manajemen Akun	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-AC-2.i	AC-2.I Manajemen Akun	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.i	AC-2.I Manajemen Akun	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.i	AC-2.I Manajemen Akun	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
CCCS-FPBMM-AC-2.i	AC-2.I Manajemen Akun	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.i	AC-2.I Manajemen Akun	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.i	AC-2.I Manajemen Akun	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.i	AC-2.I Manajemen Akun	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensi yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.i	AC-2.I Manajemen Akun	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.j	AC-2.J Manajemen Akun	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.j	AC-2.J Manajemen Akun	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.j	AC-2.J Manajemen Akun	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.j	AC-2.J Manajemen Akun	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.j	AC-2.J Manajemen Akun	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
CCCS-FPBMM-AC-2.j	AC-2.J Manajemen Akun	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.j	AC-2.J Manajemen Akun	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-AC-2.j	AC-2.J Manajemen Akun	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.j	AC-2.J Manajemen Akun	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.j	AC-2.J Manajemen Akun	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
CCCS-FPBMM-AC-2.j	AC-2.J Manajemen Akun	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.j	AC-2.J Manajemen Akun	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.j	AC-2.J Manajemen Akun	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.j	AC-2.J Manajemen Akun	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensi yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.j	AC-2.J Manajemen Akun	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.K	AC-2.K Manajemen Akun	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.K	AC-2.K Manajemen Akun	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.K	AC-2.K Manajemen Akun	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.K	AC-2.K Manajemen Akun	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.K	AC-2.K Manajemen Akun	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
CCCS-FPBMM-AC-2.K	AC-2.K Manajemen Akun	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.K	AC-2.K Manajemen Akun	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-AC-2.K	AC-2.K Manajemen Akun	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.K	AC-2.K Manajemen Akun	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.K	AC-2.K Manajemen Akun	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
CCCS-FPBMM-AC-2.K	AC-2.K Manajemen Akun	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.K	AC-2.K Manajemen Akun	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.K	AC-2.K Manajemen Akun	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.K	AC-2.K Manajemen Akun	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensi yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-2.K	AC-2.K Manajemen Akun	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensi yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-3.A	Penegakan Akses AC-3.A	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
CCCS-FPBMM-AC-4 (21)	AC-4 (21) Penegakan Arus Informasi | Pemisahan Fisik/Logis Arus Informasi	alb-http-to-https-pemeriksaan-pengalihan	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-4 (21)	AC-4 (21) Penegakan Arus Informasi | Pemisahan Fisik/Log is Arus Informasi	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
CCCS-FPBMM-AC-4 (21)	AC-4 (21) Penegakan Arus Informasi | Pemisahan Fisik/Log is Arus Informasi	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-n ode enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkrip si memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-4 (21)	AC-4 (21) Penegakan Arus Informasi | Pemisahan Fisik/Log is Arus Informasi	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-4 (21)	AC-4 (21) Penegakan Arus Informasi | Pemisahan Fisik/Logis Arus Informasi	elb-predefined-security-policy-ssl-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa pendengar SSL Classic Elastic Load Balancing Anda menggunakan kebijakan keamanan yang telah ditentukan sebelumnya. Elastic Load Balancing menyediakan konfigurasi negosiasi SSL yang telah ditentukan sebelumnya yang digunakan untuk negosiasi SSL ketika koneksi dibuat antara klien dan penyeimbang beban Anda. Konfigurasi negosiasi SSL memberikan kompatibilitas dengan berbagai klien dan menggunakan algoritma kriptografi berkekuatan tinggi. Aturan ini mengharuskan Anda menetapkan kebijakan keamanan yang telah ditentuka

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			n untuk pendengar SSL Anda. Kebijakan keamanan default adalah: ELBSecurity Policy-TLS-1-2-2017-0. Nilai aktual harus mencerminkan kebijakan organisasi Anda
CCCS-FPBMM-AC-4 (21)	AC-4 (21) Penegakan Arus Informasi | Pemisahan Fisik/Logis Arus Informasi	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-4 (21)	AC-4 (21) Penegakan Arus Informasi | Pemisahan Fisik/Logis Arus Informasi	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
CCCS-FPBMM-AC-4 (21)	AC-4 (21) Penegakan Arus Informasi | Pemisahan Fisik/Logis Arus Informasi	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-4 (21)	AC-4 (21) Penegakan Arus Informasi | Pemisahan Fisik/Logis Arus Informasi	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	alb-http-to-https-pemeriksaan-pengalihan	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	elb-predefined-security-policy-ssl-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa pendengar SSL Classic Elastic Load Balancing Anda menggunakan kebijakan keamanan yang telah ditentukan sebelumnya. Elastic Load Balancing menyediakan konfigurasi negosiasi SSL yang telah ditentukan sebelumnya yang digunakan untuk negosiasi SSL ketika koneksi dibuat antara klien dan penyeimbang beban Anda. Konfigurasi negosiasi SSL memberikan kompatibilitas dengan berbagai klien dan menggunakan algoritma kriptografi berkekuatan tinggi. Aturan ini mengharuskan Anda menetapkan kebijakan keamanan yang telah ditentuka

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			n untuk pendengar SSL Anda. Kebijakan keamanan default adalah: ELBSecurity Policy-TLS-1-2-2017-0. Nilai aktual harus mencerminkan kebijakan organisasi Anda
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-4.A	AC-4.A Penegakan Arus Informasi	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-5.A	AC-5.A Pemisahan Tugas	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-5.A	AC-5.A Pemisahan Tugas	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-5.A	AC-5.A Pemisahan Tugas	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-5.A	AC-5.A Pemisahan Tugas	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-AC-5.A	AC-5.A Pemisahan Tugas	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6 (1)	AC-6 (1) Hak Istimewa Terkecil | Otorisasi Akses ke Fungsi Keamanan	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6 (1)	AC-6 (1) Hak Istimewa Terkecil | Otorisasi Akses ke Fungsi Keamanan	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6 (1)	AC-6 (1) Hak Istimewa Terkecil | Otorisasi Akses ke Fungsi Keamanan	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6 (1)	AC-6 (1) Hak Istimewa Terkecil | Otorisasi Akses ke Fungsi Keamanan	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6 (1)	AC-6 (1) Hak Istimewa Terkecil | Otorisasi Akses ke Fungsi Keamanan	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6 (2)	AC-6 (2) Hak Istimewa Terkecil | Akses Non-Hak Istimewa untuk Fungsi Non-Keamanan	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6 (2)	AC-6 (2) Hak Istimewa Terkecil | Akses Non-Hak Istimewa untuk Fungsi Non-Keamanan	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6 (2)	AC-6 (2) Hak Istimewa Terkecil | Akses Non-Hak Istimewa untuk Fungsi Non-Keamanan	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6 (2)	AC-6 (2) Hak Istimewa Terkecil | Akses Non-Hak Istimewa untuk Fungsi Non-Keamanan	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6 (2)	AC-6 (2) Hak Istimewa Terkecil | Akses Non-Hak Istimewa untuk Fungsi Non-Keamanan	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6 (5)	AC-6 (5) Hak Istimewa Terkecil | Akun Istimewa	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6 (5)	AC-6 (5) Hak Istimewa Terkecil | Akun Istimewa	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6 (5)	AC-6 (5) Hak Istimewa Terkecil | Akun Istimewa	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6 (5)	AC-6 (5) Hak Istimewa Terkecil | Akun Istimewa	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
CCCS-FPBMM-AC-6 (9)	AC-6 (9) Hak Istimewa Terkecil | Audit Penggunaan Fungsi Istimewa	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6 (9)	AC-6 (9) Hak Istimewa Terkecil | Audit Penggunaan Fungsi Istimewa	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
CCCS-FPBMM-AC-6 (9)	AC-6 (9) Hak Istimewa Terkecil | Audit Penggunaan Fungsi Istimewa	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6 (9)	AC-6 (9) Hak Istimewa Terkecil | Audit Penggunaan Fungsi Istimewa	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6 (9)	AC-6 (9) Hak Istimewa Terkecil | Audit Penggunaan Fungsi Istimewa	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6 (9)	AC-6 (9) Hak Istimewa Terkecil | Audit Penggunaan Fungsi Istimewa	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6 (9)	AC-6 (9) Hak Istimewa Terkecil | Audit Penggunaan Fungsi Istimewa	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6 (10)	AC-6 (10) Hak Istimewa Terkecil | Melarang Pengguna yang Tidak Berhak Istimewa Menjalankan Fungsi Istimewa	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6 (10)	AC-6 (10) Hak Istimewa Terkecil | Melarang Pengguna yang Tidak Berhak Istimewa Menjalankan Fungsi Istimewa	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6 (10)	AC-6 (10) Hak Istimewa Terkecil | Melarang Pengguna yang Tidak Berhak Istimewa Menjalankan Fungsi Istimewa	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6 (10)	AC-6 (10) Hak Istimewa Terkecil | Melarang Pengguna yang Tidak Berhak Istimewa Menjalankan Fungsi Istimewa	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6 (10)	AC-6 (10) Hak Istimewa Terkecil | Melarang Pengguna yang Tidak Berhak Istimewa Menjalankan Fungsi Istimewa	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensi yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-6.A	AC-6.A Hak Istimewa Terkecil	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	api-gw-execution-l ogging-diaktifkan	Pencatatan API Gateway menampilk an tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (1)	AC-17 (1) Akses Jarak Jauh | Pemantauan/Kontrol Otomatis	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (2)	AC-17 (2) Remote Access | Perlindungan Kerahasiaan/Integritas menggunakan Enkripsi	alb-http-to-https-pemeriksaan-pengalihan	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
CCCS-FPBMM-AC-17 (2)	AC-17 (2) Remote Access | Perlindungan Kerahasiaan/Integritas menggunakan Enkripsi	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (2)	AC-17 (2) Remote Access | Perlindungan Kerahasiaan/Integritas menggunakan Enkripsi	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (2)	AC-17 (2) Remote Access | Perlindungan Kerahasiaan/Integritas menggunakan Enkripsi	elb-predefined-security-policy-ssl-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa pendengar SSL Classic Elastic Load Balancing Anda menggunakan kebijakan keamanan yang telah ditentukan sebelumnya. Elastic Load Balancing menyediakan konfigurasi negosiasi SSL yang telah ditentukan sebelumnya yang digunakan untuk negosiasi SSL ketika koneksi dibuat antara klien dan penyeimbang beban Anda. Konfigurasi negosiasi SSL memberikan kompatibilitas dengan berbagai klien dan menggunakan algoritma kriptografi berkekuatan tinggi. Aturan ini mengharuskan Anda menetapkan kebijakan keamanan yang telah ditentuka

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			n untuk pendengar SSL Anda. Kebijakan keamanan default adalah: ELBSecurity Policy-TLS-1-2-2017-0. Nilai aktual harus mencerminkan kebijakan organisasi Anda
CCCS-FPBMM-AC-17 (2)	AC-17 (2) Remote Access | Perlindungan Kerahasiaan/Integritas menggunakan Enkripsi	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (2)	AC-17 (2) Remote Access | Perlindungan Kerahasiaan/Integritas menggunakan Enkripsi	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (3)	AC-17 (3) Akses Jarak Jauh | Titik Kontrol Akses Terkelola	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (4)	AC-17 (4) Akses Jarak Jauh | Perintah/ Akses Istimewa	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (4)	AC-17 (4) Akses Jarak Jauh | Perintah/ Akses Istimewa	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17 (4)	AC-17 (4) Akses Jarak Jauh | Perintah/ Akses Istimewa	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
CCCS-FPBMM-AC-17.A	AC-17.A Akses Jarak Jauh	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.A	AC-17.A Akses Jarak Jauh	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-AC-17.A	AC-17.A Akses Jarak Jauh	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.A	AC-17.A Akses Jarak Jauh	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
CCCS-FPBMM-AC-17.A	AC-17.A Akses Jarak Jauh	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.A	AC-17.A Akses Jarak Jauh	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.A	AC-17.A Akses Jarak Jauh	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.A	AC-17.A Akses Jarak Jauh	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
CCCS-FPBMM-AC-17.A	AC-17.A Akses Jarak Jauh	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.A	AC-17.A Akses Jarak Jauh	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.A	AC-17.A Akses Jarak Jauh	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.A	AC-17.A Akses Jarak Jauh	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-AC-17.A	AC-17.A Akses Jarak Jauh	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.A	AC-17.A Akses Jarak Jauh	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.A	AC-17.A Akses Jarak Jauh	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.A	AC-17.A Akses Jarak Jauh	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.A	AC-17.A Akses Jarak Jauh	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
CCCS-FPBMM-AC-17.A	AC-17.A Akses Jarak Jauh	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.A	AC-17.A Akses Jarak Jauh	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
CCCS-FPBMM-AC-17.A	AC-17.A Akses Jarak Jauh	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.A	AC-17.A Akses Jarak Jauh	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.A	AC-17.A Akses Jarak Jauh	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.A	AC-17.A Akses Jarak Jauh	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.AA	Akses Jarak Jauh AC-17.AA	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-AC-17.AA	Akses Jarak Jauh AC-17.AA	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-AC-17.AA	Akses Jarak Jauh AC-17.AA	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.AA	Akses Jarak Jauh AC-17.AA	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
CCCS-FPBMM-AC-17.AA	Akses Jarak Jauh AC-17.AA	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.AA	Akses Jarak Jauh AC-17.AA	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.AA	Akses Jarak Jauh AC-17.AA	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.AA	Akses Jarak Jauh AC-17.AA	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
CCCS-FPBMM-AC-17.AA	Akses Jarak Jauh AC-17.AA	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.AA	Akses Jarak Jauh AC-17.AA	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.AA	Akses Jarak Jauh AC-17.AA	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.AA	Akses Jarak Jauh AC-17.AA	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-AC-17.AA	Akses Jarak Jauh AC-17.AA	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.AA	Akses Jarak Jauh AC-17.AA	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.AA	Akses Jarak Jauh AC-17.AA	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.AA	Akses Jarak Jauh AC-17.AA	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.AA	Akses Jarak Jauh AC-17.AA	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
CCCS-FPBMM-AC-17.AA	Akses Jarak Jauh AC-17.AA	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.AA	Akses Jarak Jauh AC-17.AA	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
CCCS-FPBMM-AC-17.AA	Akses Jarak Jauh AC-17.AA	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.AA	Akses Jarak Jauh AC-17.AA	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.AA	Akses Jarak Jauh AC-17.AA	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.AA	Akses Jarak Jauh AC-17.AA	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.b	Akses Jarak Jauh AC-17.B	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-AC-17.b	Akses Jarak Jauh AC-17.B	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-AC-17.b	Akses Jarak Jauh AC-17.B	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.b	Akses Jarak Jauh AC-17.B	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
CCCS-FPBMM-AC-17.b	Akses Jarak Jauh AC-17.B	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.b	Akses Jarak Jauh AC-17.B	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.b	Akses Jarak Jauh AC-17.B	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.b	Akses Jarak Jauh AC-17.B	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
CCCS-FPBMM-AC-17.b	Akses Jarak Jauh AC-17.B	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.b	Akses Jarak Jauh AC-17.B	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.b	Akses Jarak Jauh AC-17.B	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.b	Akses Jarak Jauh AC-17.B	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-AC-17.b	Akses Jarak Jauh AC-17.B	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.b	Akses Jarak Jauh AC-17.B	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.b	Akses Jarak Jauh AC-17.B	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.b	Akses Jarak Jauh AC-17.B	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.b	Akses Jarak Jauh AC-17.B	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
CCCS-FPBMM-AC-17.b	Akses Jarak Jauh AC-17.B	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.b	Akses Jarak Jauh AC-17.B	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
CCCS-FPBMM-AC-17.b	Akses Jarak Jauh AC-17.B	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.b	Akses Jarak Jauh AC-17.B	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.b	Akses Jarak Jauh AC-17.B	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AC-17.b	Akses Jarak Jauh AC-17.B	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.A	Acara Audit AU-2.A	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
CCCS-FPBMM-AU-2.A	Acara Audit AU-2.A	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.A	Acara Audit AU-2.A	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
CCCS-FPBMM-AU-2.A	Acara Audit AU-2.A	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.A	Acara Audit AU-2.A	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.A	Acara Audit AU-2.A	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.A	Acara Audit AU-2.A	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.A	Acara Audit AU-2.A	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDbEncrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.A	Acara Audit AU-2.A	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.A	Acara Audit AU-2.A	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.A	Acara Audit AU-2.A	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
CCCS-FPBMM-AU-2.B	Acara Audit AU-2.B	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.B	Acara Audit AU-2.B	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
CCCS-FPBMM-AU-2.B	Acara Audit AU-2.B	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.B	Acara Audit AU-2.B	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.B	Acara Audit AU-2.B	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.B	Acara Audit AU-2.B	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.B	Acara Audit AU-2.B	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.B	Acara Audit AU-2.B	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDbEncrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.B	Acara Audit AU-2.B	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.B	Acara Audit AU-2.B	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.B	Acara Audit AU-2.B	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
CCCS-FPBMM-AU-2.c	Acara Audit AU-2.C	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.c	Acara Audit AU-2.C	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
CCCS-FPBMM-AU-2.c	Acara Audit AU-2.C	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.c	Acara Audit AU-2.C	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.c	Acara Audit AU-2.C	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.c	Acara Audit AU-2.C	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.c	Acara Audit AU-2.C	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.c	Acara Audit AU-2.C	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.c	Acara Audit AU-2.C	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.c	Acara Audit AU-2.C	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.c	Acara Audit AU-2.C	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
CCCS-FPBMM-AU-2.D	Acara Audit AU-2.D	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.D	Acara Audit AU-2.D	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
CCCS-FPBMM-AU-2.D	Acara Audit AU-2.D	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.D	Acara Audit AU-2.D	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.D	Acara Audit AU-2.D	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.D	Acara Audit AU-2.D	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.D	Acara Audit AU-2.D	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.D	Acara Audit AU-2.D	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDbEncrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.D	Acara Audit AU-2.D	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.D	Acara Audit AU-2.D	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-2.D	Acara Audit AU-2.D	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
CCCS-FPBMM-AU-3 (1)	AU-3 (1) Isi Catatan Audit | Informasi Audit Tambahan	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-3 (1)	AU-3 (1) Isi Catatan Audit | Informasi Audit Tambahan	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
CCCS-FPBMM-AU-3 (1)	AU-3 (1) Isi Catatan Audit | Informasi Audit Tambahan	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-3 (1)	AU-3 (1) Isi Catatan Audit | Informasi Audit Tambahan	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-3 (1)	AU-3 (1) Isi Catatan Audit | Informasi Audit Tambahan	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-3 (1)	AU-3 (1) Isi Catatan Audit | Informasi Audit Tambahan	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-3 (1)	AU-3 (1) Isi Catatan Audit | Informasi Audit Tambahan	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-3 (1)	AU-3 (1) Isi Catatan Audit | Informasi Audit Tambahan	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-3.A	AU-3.A Isi Catatan Audit	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
CCCS-FPBMM-AU-3.A	AU-3.A Isi Catatan Audit	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-3.A	AU-3.A Isi Catatan Audit	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
CCCS-FPBMM-AU-3.A	AU-3.A Isi Catatan Audit	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-3.A	AU-3.A Isi Catatan Audit	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-3.A	AU-3.A Isi Catatan Audit	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-3.A	AU-3.A Isi Catatan Audit	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-3.A	AU-3.A Isi Catatan Audit	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-3.A	AU-3.A Isi Catatan Audit	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-3.A	AU-3.A Isi Catatan Audit	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDbEncrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-3.A	AU-3.A Isi Catatan Audit	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-3.A	AU-3.A Isi Catatan Audit	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-3.A	AU-3.A Isi Catatan Audit	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-5.A	AU-5.A Respon terhadap Kegagalan Pemrosesan Audit	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai sebenarnya harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-5.B	AU-5.B Respon terhadap Kegagalan Pemrosesan Audit	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai sebenarnya harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-6 (1)	AU-6 (1) Tinjauan Audit, Analisis, dan Pelaporan | Integrasi Proses	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai sebenarnya harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-6 (1)	AU-6 (1) Tinjauan Audit, Analisis, dan Pelaporan | Integrasi Proses	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
CCCS-FPBMM-AU-6 (1)	AU-6 (1) Tinjauan Audit, Analisis, dan Pelaporan | Integrasi Proses	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-6 (1)	AU-6 (1) Tinjauan Audit, Analisis, dan Pelaporan | Integrasi Proses	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-6 (1)	AU-6 (1) Tinjauan Audit, Analisis, dan Pelaporan | Integrasi Proses	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-6 (1)	AU-6 (1) Tinjauan Audit, Analisis, dan Pelaporan | Integrasi Proses	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-6 (3)	AU-6 (3) Tinjauan Audit, Analisis, dan Pelaporan | Repositori Audit Berkorelasi	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
CCCS-FPBMM-AU-6 (3)	AU-6 (3) Tinjauan Audit, Analisis, dan Pelaporan | Repositori Audit Berkorelasi	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-6 (3)	AU-6 (3) Tinjauan Audit, Analisis, dan Pelaporan | Repositori Audit Berkorelasi	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
CCCS-FPBMM-AU-6 (3)	AU-6 (3) Tinjauan Audit, Analisis, dan Pelaporan | Repositori Audit Berkorelasi	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-6 (3)	AU-6 (3) Tinjauan Audit, Analisis, dan Pelaporan | Repositori Audit Berkorelasi	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-6 (3)	AU-6 (3) Tinjauan Audit, Analisis, dan Pelaporan | Repositori Audit Berkorelasi	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.
CCCS-FPBMM-AU-6 (3)	AU-6 (3) Tinjauan Audit, Analisis, dan Pelaporan | Repositori Audit Berkorelasi	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-6 (3)	AU-6 (3) Tinjauan Audit, Analisis, dan Pelaporan | Repositori Audit Berkorelasi	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-6 (3)	AU-6 (3) Tinjauan Audit, Analisis, dan Pelaporan | Repositori Audit Berkorelasi	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-6 (3)	AU-6 (3) Tinjauan Audit, Analisis, dan Pelaporan | Repositori Audit Berkorelasi	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-6 (3)	AU-6 (3) Tinjauan Audit, Analisis, dan Pelaporan | Repositori Audit Berkorelasi	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-6 (3)	AU-6 (3) Tinjauan Audit, Analisis, dan Pelaporan | Repositori Audit Berkorelasi	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-6 (3)	AU-6 (3) Tinjauan Audit, Analisis, dan Pelaporan | Repositori Audit Berkorelasi	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-6 (3)	AU-6 (3) Tinjauan Audit, Analisis, dan Pelaporan | Repositori Audit Berkorelasi	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-6 (3)	AU-6 (3) Tinjauan Audit, Analisis, dan Pelaporan | Repositori Audit Berkorelasi	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
CCCS-FPBMM-AU-7 (1)	AU-7 (1) Pengurangan Audit dan Pembuatan Laporan | Pemrosesan Otomatis	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-8.B	AU-8.B Perangko Waktu	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
CCCS-FPBMM-AU-8.B	AU-8.B Perangko Waktu	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-8.B	AU-8.B Perangko Waktu	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
CCCS-FPBMM-AU-8.B	AU-8.B Perangko Waktu	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-8.B	AU-8.B Perangko Waktu	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-8.B	AU-8.B Perangko Waktu	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-8.B	AU-8.B Perangko Waktu	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-8.B	AU-8.B Perangko Waktu	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-8.B	AU-8.B Perangko Waktu	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-8.B	AU-8.B Perangko Waktu	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDbEncrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-8.B	AU-8.B Perangko Waktu	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-8.B	AU-8.B Perangko Waktu	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-8.B	AU-8.B Perangko Waktu	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-9 (2)	AU-9 (2) Perlindungan Informasi Audit | Audit Backup pada Sistem/Komponen Fisik Terpisah	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-9 (2)	AU-9 (2) Perlindungan Informasi Audit | Audit Backup pada Sistem/Komponen Fisik Terpisah	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-9 (2)	AU-9 (2) Perlindungan Informasi Audit | Audit Backup pada Sistem/Komponen Fisik Terpisah	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.
CCCS-FPBMM-AU-9.A	AU-9.A Perlindungan Informasi Audit	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-9.A	AU-9.A Perlindungan Informasi Audit	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-9.A	AU-9.A Perlindungan Informasi Audit	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
CCCS-FPBMM-AU-11.A	AU-11.A Retensi Catatan Audit	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-11.B	Retensi Catatan Audit AU-11.B	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.
CCCS-FPBMM-AU-11.c	Retensi Catatan Audit AU-11.C	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-12.A	Generasi Audit AU-12.A	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
CCCS-FPBMM-AU-12.A	Generasi Audit AU-12.A	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-12.A	Generasi Audit AU-12.A	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
CCCS-FPBMM-AU-12.A	Generasi Audit AU-12.A	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-12.A	Generasi Audit AU-12.A	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-12.A	Generasi Audit AU-12.A	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-12.A	Generasi Audit AU-12.A	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-12.A	Generasi Audit AU-12.A	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-12.A	Generasi Audit AU-12.A	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-12.A	Generasi Audit AU-12.A	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-12.A	Generasi Audit AU-12.A	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-12.A	Generasi Audit AU-12.A	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-12.A	Generasi Audit AU-12.A	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
CCCS-FPBMM-AU-12.c	Generasi Audit AU-12.C	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-12.c	Generasi Audit AU-12.C	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
CCCS-FPBMM-AU-12.c	Generasi Audit AU-12.C	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-12.c	Generasi Audit AU-12.C	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-12.c	Generasi Audit AU-12.C	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-12.c	Generasi Audit AU-12.C	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-12.c	Generasi Audit AU-12.C	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-12.c	Generasi Audit AU-12.C	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-12.c	Generasi Audit AU-12.C	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-12.c	Generasi Audit AU-12.C	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-AU-12.c	Generasi Audit AU-12.C	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
CCCS-FPBMM-CA-3 (5)	CA-3 (5) Interkoneksi Sistem | Pembatasan Koneksi Jaringan Eksternal	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-3 (5)	CA-3 (5) Interkoneksi Sistem | Pembatasan Koneksi Jaringan Eksternal	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-CA-3 (5)	CA-3 (5) Interkoneksi Sistem | Pembatasan Koneksi Jaringan Eksternal	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-3 (5)	CA-3 (5) Interkoneksi Sistem | Pembatasan Koneksi Jaringan Eksternal	terlampir eip	Aturan ini memastikan Elastic IPs dialokasikan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan. Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-3 (5)	CA-3 (5) Interkoneksi Sistem | Pembatasan Koneksi Jaringan Eksternal	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
CCCS-FPBMM-CA-3 (5)	CA-3 (5) Interkoneksi Sistem | Pembatasan Koneksi Jaringan Eksternal	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-3 (5)	CA-3 (5) Interkoneksi Sistem | Pembatasan Koneksi Jaringan Eksternal	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-3 (5)	CA-3 (5) Interkoneksi Sistem | Pembatasan Koneksi Jaringan Eksternal	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-3 (5)	CA-3 (5) Interkoneksi Sistem | Pembatasan Koneksi Jaringan Eksternal	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
CCCS-FPBMM-CA-3 (5)	CA-3 (5) Interkoneksi Sistem | Pembatasan Koneksi Jaringan Eksternal	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-3 (5)	CA-3 (5) Interkoneksi Sistem | Pembatasan Koneksi Jaringan Eksternal	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigurasi ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-3 (5)	CA-3 (5) Interkoneksi Sistem | Pembatasan Koneksi Jaringan Eksternal	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-3 (5)	CA-3 (5) Interkoneksi Sistem | Pembatasan Koneksi Jaringan Eksternal	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-CA-3 (5)	CA-3 (5) Interkoneksi Sistem | Pembatasan Koneksi Jaringan Eksternal	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-3 (5)	CA-3 (5) Interkoneksi Sistem | Pembatasan Koneksi Jaringan Eksternal	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-3 (5)	CA-3 (5) Interkoneksi Sistem | Pembatasan Koneksi Jaringan Eksternal	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-3 (5)	CA-3 (5) Interkoneksi Sistem | Pembatasan Koneksi Jaringan Eksternal	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-3 (5)	CA-3 (5) Interkoneksi Sistem | Pembatasan Koneksi Jaringan Eksternal	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
CCCS-FPBMM-CA-3 (5)	CA-3 (5) Interkoneksi Sistem | Pembatasan Koneksi Jaringan Eksternal	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-3 (5)	CA-3 (5) Interkoneksi Sistem | Pembatasan Koneksi Jaringan Eksternal	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
CCCS-FPBMM-CA-3 (5)	CA-3 (5) Interkoneksi Sistem | Pembatasan Koneksi Jaringan Eksternal	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-3 (5)	CA-3 (5) Interkoneksi Sistem | Pembatasan Koneksi Jaringan Eksternal	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-3 (5)	CA-3 (5) Interkoneksi Sistem | Pembatasan Koneksi Jaringan Eksternal	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-3 (5)	CA-3 (5) Interkoneksi Sistem | Pembatasan Koneksi Jaringan Eksternal	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.A	CA-7.A Pemantauan Berkelanjutan	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.A	CA-7.A Pemantauan Berkelanjutan	api-gw-xray-enabled	AWS X-Ray mengumpulkan data tentang permintaan yang disajikan aplikasi Anda, dan menyediakan alat yang dapat Anda gunakan untuk melihat, memfilter , dan mendapatkan wawasan tentang data tersebut guna mengidentifikasi masalah dan peluang pengoptimalan. Pastikan X-Ray diaktifkan sehingga Anda dapat melihat informasi terperinci tidak hanya tentang permintaan dan respons, tetapi juga tentang panggilan yang dilakukan aplikasi Anda ke AWS sumber daya hilir, layanan mikro, database, dan web HTTP. APIs

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.A	CA-7.A Pemantauan Berkelanjutan	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.A	CA-7.A Pemantauan Berkelanjutan	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.A	CA-7.A Pemantauan Berkelanjutan	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.A	CA-7.A Pemantauan Berkelanjutan	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai sebenarnya harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.A	CA-7.A Pemantauan Berkelanjutan	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
CCCS-FPBMM-CA-7.A	CA-7.A Pemantauan Berkelanjutan	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.A	CA-7.A Pemantauan Berkelanjutan	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.A	CA-7.A Pemantauan Berkelanjutan	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-CA-7.A	CA-7.A Pemantauan Berkelanjutan	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.A	CA-7.A Pemantauan Berkelanjutan	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.
CCCS-FPBMM-CA-7.A	CA-7.A Pemantauan Berkelanjutan	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.A	CA-7.A Pemantauan Berkelanjutan	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.A	CA-7.A Pemantauan Berkelanjutan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.A	CA-7.A Pemantauan Berkelanjutan	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.A	CA-7.A Pemantauan Berkelanjutan	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.A	CA-7.A Pemantauan Berkelanjutan	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.A	CA-7.A Pemantauan Berkelanjutan	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.A	CA-7.A Pemantauan Berkelanjutan	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.A	CA-7.A Pemantauan Berkelanjutan	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.A	CA-7.A Pemantauan Berkelanjutan	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.A	CA-7.A Pemantauan Berkelanjutan	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.A	CA-7.A Pemantauan Berkelanjutan	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.A	CA-7.A Pemantauan Berkelanjutan	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
CCCS-FPBMM-CA-7.b	CA-7.B Pemantauan Berkelanjutan	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.b	CA-7.B Pemantauan Berkelanjutan	api-gw-xray-enabled	AWS X-Ray mengumpulkan data tentang permintaan yang disajikan aplikasi Anda, dan menyediakan alat yang dapat Anda gunakan untuk melihat, memfilter, dan mendapatkan wawasan tentang data tersebut guna mengidentifikasi masalah dan peluang pengoptimalan. Pastikan X-Ray diaktifkan sehingga Anda dapat melihat informasi terperinci tidak hanya tentang permintaan dan respons, tetapi juga tentang panggilan yang dilakukan aplikasi Anda ke AWS sumber daya hilir, layanan mikro, database, dan web HTTP. APIs

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.b	CA-7.B Pemantauan Berkelanjutan	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.b	CA-7.B Pemantauan Berkelanjutan	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.b	CA-7.B Pemantauan Berkelanjutan	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.b	CA-7.B Pemantauan Berkelanjutan	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai sebenarnya harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.b	CA-7.B Pemantauan Berkelanjutan	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
CCCS-FPBMM-CA-7.b	CA-7.B Pemantauan Berkelanjutan	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.b	CA-7.B Pemantauan Berkelanjutan	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.b	CA-7.B Pemantauan Berkelanjutan	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-CA-7.b	CA-7.B Pemantauan Berkelanjutan	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.b	CA-7.B Pemantauan Berkelanjutan	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.b	CA-7.B Pemantauan Berkelanjutan	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.b	CA-7.B Pemantauan Berkelanjutan	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
CCCS-FPBMM-CA-7.b	CA-7.B Pemantauan Berkelanjutan	terlampir eip	Aturan ini memastikan Elastic IPs dialokasikan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan. Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.b	CA-7.B Pemantauan Berkelanjutan	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.b	CA-7.B Pemantauan Berkelanjutan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.b	CA-7.B Pemantauan Berkelanjutan	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.b	CA-7.B Pemantauan Berkelanjutan	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.b	CA-7.B Pemantauan Berkelanjutan	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.b	CA-7.B Pemantauan Berkelanjutan	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.b	CA-7.B Pemantauan Berkelanjutan	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.b	CA-7.B Pemantauan Berkelanjutan	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.b	CA-7.B Pemantauan Berkelanjutan	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.b	CA-7.B Pemantauan Berkelanjutan	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.b	CA-7.B Pemantauan Berkelanjutan	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.b	CA-7.B Pemantauan Berkelanjutan	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
CCCS-FPBMM-CA-7.c	CA-7.C Pemantauan Berkelanjutan	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.c	CA-7.C Pemantauan Berkelanjutan	api-gw-xray-enabled	AWS X-Ray mengumpulkan data tentang permintaan yang disajikan aplikasi Anda, dan menyediakan alat yang dapat Anda gunakan untuk melihat, memfilter , dan mendapatkan wawasan tentang data tersebut guna mengidentifikasi masalah dan peluang pengoptimalan. Pastikan X-Ray diaktifkan sehingga Anda dapat melihat informasi terperinci tidak hanya tentang permintaan dan respons, tetapi juga tentang panggilan yang dilakukan aplikasi Anda ke AWS sumber daya hilir, layanan mikro, database, dan web HTTP. APIs

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.c	CA-7.C Pemantauan Berkelanjutan	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.c	CA-7.C Pemantauan Berkelanjutan	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.c	CA-7.C Pemantauan Berkelanjutan	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.c	CA-7.C Pemantauan Berkelanjutan	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai sebenarnya harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.c	CA-7.C Pemantauan Berkelanjutan	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
CCCS-FPBMM-CA-7.c	CA-7.C Pemantauan Berkelanjutan	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.c	CA-7.C Pemantauan Berkelanjutan	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.c	CA-7.C Pemantauan Berkelanjutan	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-CA-7.c	CA-7.C Pemantauan Berkelanjutan	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.c	CA-7.C Pemantauan Berkelanjutan	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.c	CA-7.C Pemantauan Berkelanjutan	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.c	CA-7.C Pemantauan Berkelanjutan	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
CCCS-FPBMM-CA-7.c	CA-7.C Pemantauan Berkelanjutan	terlampir eip	Aturan ini memastikan Elastic IPs dialokasikan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan. Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.c	CA-7.C Pemantauan Berkelanjutan	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.c	CA-7.C Pemantauan Berkelanjutan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.c	CA-7.C Pemantauan Berkelanjutan	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.c	CA-7.C Pemantauan Berkelanjutan	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.c	CA-7.C Pemantauan Berkelanjutan	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.c	CA-7.C Pemantauan Berkelanjutan	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.c	CA-7.C Pemantauan Berkelanjutan	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.c	CA-7.C Pemantauan Berkelanjutan	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.c	CA-7.C Pemantauan Berkelanjutan	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.c	CA-7.C Pemantauan Berkelanjutan	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.c	CA-7.C Pemantauan Berkelanjutan	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.c	CA-7.C Pemantauan Berkelanjutan	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
CCCS-FPBMM-CA-7.d	CA-7.D Pemantauan Berkelanjutan	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.d	CA-7.D Pemantauan Berkelanjutan	api-gw-xray-enabled	AWS X-Ray mengumpulkan data tentang permintaan yang disajikan aplikasi Anda, dan menyediakan alat yang dapat Anda gunakan untuk melihat, memfilter , dan mendapatkan wawasan tentang data tersebut guna mengidentifikasi masalah dan peluang pengoptimalan. Pastikan X-Ray diaktifkan sehingga Anda dapat melihat informasi terperinci tidak hanya tentang permintaan dan respons, tetapi juga tentang panggilan yang dilakukan aplikasi Anda ke AWS sumber daya hilir, layanan mikro, database, dan web HTTP. APIs

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.d	CA-7.D Pemantauan Berkelanjutan	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.d	CA-7.D Pemantauan Berkelanjutan	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.d	CA-7.D Pemantauan Berkelanjutan	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.d	CA-7.D Pemantauan Berkelanjutan	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai sebenarnya harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.d	CA-7.D Pemantauan Berkelanjutan	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
CCCS-FPBMM-CA-7.d	CA-7.D Pemantauan Berkelanjutan	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.d	CA-7.D Pemantauan Berkelanjutan	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.d	CA-7.D Pemantauan Berkelanjutan	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-CA-7.d	CA-7.D Pemantauan Berkelanjutan	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.d	CA-7.D Pemantauan Berkelanjutan	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.d	CA-7.D Pemantauan Berkelanjutan	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.d	CA-7.D Pemantauan Berkelanjutan	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
CCCS-FPBMM-CA-7.d	CA-7.D Pemantauan Berkelanjutan	terlampir eip	Aturan ini memastikan Elastic IPs dialokasikan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan. Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.d	CA-7.D Pemantauan Berkelanjutan	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.d	CA-7.D Pemantauan Berkelanjutan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.d	CA-7.D Pemantauan Berkelanjutan	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.d	CA-7.D Pemantauan Berkelanjutan	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.d	CA-7.D Pemantauan Berkelanjutan	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.d	CA-7.D Pemantauan Berkelanjutan	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.d	CA-7.D Pemantauan Berkelanjutan	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.d	CA-7.D Pemantauan Berkelanjutan	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.d	CA-7.D Pemantauan Berkelanjutan	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.d	CA-7.D Pemantauan Berkelanjutan	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.d	CA-7.D Pemantauan Berkelanjutan	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.d	CA-7.D Pemantauan Berkelanjutan	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
CCCS-FPBMM-CA-7.e	CA-7.E Pemantauan Berkelanjutan	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.e	CA-7.E Pemantauan Berkelanjutan	api-gw-xray-enabled	AWS X-Ray mengumpulkan data tentang permintaan yang disajikan aplikasi Anda, dan menyediakan alat yang dapat Anda gunakan untuk melihat, memfilter , dan mendapatkan wawasan tentang data tersebut guna mengidentifikasi masalah dan peluang pengoptimalan. Pastikan X-Ray diaktifkan sehingga Anda dapat melihat informasi terperinci tidak hanya tentang permintaan dan respons, tetapi juga tentang panggilan yang dilakukan aplikasi Anda ke AWS sumber daya hilir, layanan mikro, database, dan web HTTP. APIs

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.e	CA-7.E Pemantauan Berkelanjutan	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.e	CA-7.E Pemantauan Berkelanjutan	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.e	CA-7.E Pemantauan Berkelanjutan	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.e	CA-7.E Pemantauan Berkelanjutan	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai sebenarnya harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.e	CA-7.E Pemantauan Berkelanjutan	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
CCCS-FPBMM-CA-7.e	CA-7.E Pemantauan Berkelanjutan	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.e	CA-7.E Pemantauan Berkelanjutan	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.e	CA-7.E Pemantauan Berkelanjutan	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-CA-7.e	CA-7.E Pemantauan Berkelanjutan	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.e	CA-7.E Pemantauan Berkelanjutan	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.e	CA-7.E Pemantauan Berkelanjutan	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.e	CA-7.E Pemantauan Berkelanjutan	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
CCCS-FPBMM-CA-7.e	CA-7.E Pemantauan Berkelanjutan	terlampir eip	Aturan ini memastikan Elastic IPs dialokasikan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan. Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.e	CA-7.E Pemantauan Berkelanjutan	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.e	CA-7.E Pemantauan Berkelanjutan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.e	CA-7.E Pemantauan Berkelanjutan	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.e	CA-7.E Pemantauan Berkelanjutan	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.e	CA-7.E Pemantauan Berkelanjutan	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.e	CA-7.E Pemantauan Berkelanjutan	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.e	CA-7.E Pemantauan Berkelanjutan	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.e	CA-7.E Pemantauan Berkelanjutan	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.e	CA-7.E Pemantauan Berkelanjutan	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.e	CA-7.E Pemantauan Berkelanjutan	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.e	CA-7.E Pemantauan Berkelanjutan	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.e	CA-7.E Pemantauan Berkelanjutan	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatata n AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
CCCS-FPBMM-CA-7.f	CA-7.F Pemantauan Berkelanjutan	api-gw-execution-l ogging-diaktifkan	Pencatatan API Gateway menampilk an tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.f	CA-7.F Pemantauan Berkelanjutan	api-gw-xray-enabled	AWS X-Ray mengumpulkan data tentang permintaan yang disajikan aplikasi Anda, dan menyediakan alat yang dapat Anda gunakan untuk melihat, memfilter, dan mendapatkan wawasan tentang data tersebut guna mengidentifikasi masalah dan peluang pengoptimalan. Pastikan X-Ray diaktifkan sehingga Anda dapat melihat informasi terperinci tidak hanya tentang permintaan dan respons, tetapi juga tentang panggilan yang dilakukan aplikasi Anda ke AWS sumber daya hilir, layanan mikro, database, dan web HTTP. APIs

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.f	CA-7.F Pemantauan Berkelanjutan	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.f	CA-7.F Pemantauan Berkelanjutan	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.f	CA-7.F Pemantauan Berkelanjutan	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.f	CA-7.F Pemantauan Berkelanjutan	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai sebenarnya harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.f	CA-7.F Pemantauan Berkelanjutan	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
CCCS-FPBMM-CA-7.f	CA-7.F Pemantauan Berkelanjutan	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.f	CA-7.F Pemantauan Berkelanjutan	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.f	CA-7.F Pemantauan Berkelanjutan	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-CA-7.f	CA-7.F Pemantauan Berkelanjutan	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.f	CA-7.F Pemantauan Berkelanjutan	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.f	CA-7.F Pemantauan Berkelanjutan	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.f	CA-7.F Pemantauan Berkelanjutan	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
CCCS-FPBMM-CA-7.f	CA-7.F Pemantauan Berkelanjutan	terlampir eip	Aturan ini memastikan Elastic IPs dialokasikan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan. Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.f	CA-7.F Pemantauan Berkelanjutan	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.f	CA-7.F Pemantauan Berkelanjutan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.f	CA-7.F Pemantauan Berkelanjutan	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.f	CA-7.F Pemantauan Berkelanjutan	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.f	CA-7.F Pemantauan Berkelanjutan	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.f	CA-7.F Pemantauan Berkelanjutan	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.f	CA-7.F Pemantauan Berkelanjutan	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.f	CA-7.F Pemantauan Berkelanjutan	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.f	CA-7.F Pemantauan Berkelanjutan	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.f	CA-7.F Pemantauan Berkelanjutan	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.f	CA-7.F Pemantauan Berkelanjutan	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.f	CA-7.F Pemantauan Berkelanjutan	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatata n AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
CCCS-FPBMM-CA-7.g	CA-7.G Pemantauan Berkelanjutan	api-gw-execution-l ogging-diaktifkan	Pencatatan API Gateway menampilk an tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.g	CA-7.G Pemantauan Berkelanjutan	api-gw-xray-enabled	AWS X-Ray mengumpulkan data tentang permintaan yang disajikan aplikasi Anda, dan menyediakan alat yang dapat Anda gunakan untuk melihat, memfilter , dan mendapatkan wawasan tentang data tersebut guna mengidentifikasi masalah dan peluang pengoptimalan. Pastikan X-Ray diaktifkan sehingga Anda dapat melihat informasi terperinci tidak hanya tentang permintaan dan respons, tetapi juga tentang panggilan yang dilakukan aplikasi Anda ke AWS sumber daya hilir, layanan mikro, database, dan web HTTP. APIs

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.g	CA-7.G Pemantauan Berkelanjutan	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.g	CA-7.G Pemantauan Berkelanjutan	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.g	CA-7.G Pemantauan Berkelanjutan	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.g	CA-7.G Pemantauan Berkelanjutan	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai sebenarnya harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.g	CA-7.G Pemantauan Berkelanjutan	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
CCCS-FPBMM-CA-7.g	CA-7.G Pemantauan Berkelanjutan	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.g	CA-7.G Pemantauan Berkelanjutan	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.g	CA-7.G Pemantauan Berkelanjutan	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-CA-7.g	CA-7.G Pemantauan Berkelanjutan	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.g	CA-7.G Pemantauan Berkelanjutan	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.g	CA-7.G Pemantauan Berkelanjutan	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.g	CA-7.G Pemantauan Berkelanjutan	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
CCCS-FPBMM-CA-7.g	CA-7.G Pemantauan Berkelanjutan	terlampir eip	Aturan ini memastikan Elastic IPs dialokasikan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan. Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.g	CA-7.G Pemantauan Berkelanjutan	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.g	CA-7.G Pemantauan Berkelanjutan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.g	CA-7.G Pemantauan Berkelanjutan	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.g	CA-7.G Pemantauan Berkelanjutan	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.g	CA-7.G Pemantauan Berkelanjutan	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.g	CA-7.G Pemantauan Berkelanjutan	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.g	CA-7.G Pemantauan Berkelanjutan	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.g	CA-7.G Pemantauan Berkelanjutan	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.g	CA-7.G Pemantauan Berkelanjutan	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.g	CA-7.G Pemantauan Berkelanjutan	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.g	CA-7.G Pemantauan Berkelanjutan	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-7.g	CA-7.G Pemantauan Berkelanjutan	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatata n AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	alb-http-to-https-pemeriksaan-pengalihan	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	elb-predefined-security-policy-ssl-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa pendengar SSL Classic Elastic Load Balancing Anda menggunakan kebijakan keamanan yang telah ditentukan sebelumnya. Elastic Load Balancing menyediakan konfigurasi negosiasi SSL yang telah ditentukan sebelumnya yang digunakan untuk negosiasi SSL ketika koneksi dibuat antara klien dan penyeimbang beban Anda. Konfigurasi negosiasi SSL memberikan kompatibilitas dengan berbagai klien dan menggunakan algoritma kriptografi berkekuatan tinggi. Aturan ini mengharuskan Anda menetapkan kebijakan keamanan yang telah ditentuka

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			n untuk pendengar SSL Anda. Kebijakan keamanan default adalah: ELBSecurity Policy-TLS-1-2-2017-0. Nilai aktual harus mencerminkan kebijakan organisasi Anda
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CA-9.A	CA-9.A Koneksi Sistem Internal	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-2.A	Konfigurasi Dasar CM-2.A	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-2.A	Konfigurasi Dasar CM-2.A	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-2.A	Konfigurasi Dasar CM-2.A	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.
CCCS-FPBMM-CM-2.A	Konfigurasi Dasar CM-2.A	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-2.A	Konfigurasi Dasar CM-2.A	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-2.A	Konfigurasi Dasar CM-2.A	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-2.A	Konfigurasi Dasar CM-2.A	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-3.A	Kontrol Perubahan Konfigurasi CM-3.A	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-3.A	Kontrol Perubahan Konfigurasi CM-3.A	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-3.b	Kontrol Perubahan Konfigurasi CM-3.B	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-3.b	Kontrol Perubahan Konfigurasi CM-3.B	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-3.c	Kontrol Perubahan Konfigurasi CM-3.C	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-3.c	Kontrol Perubahan Konfigurasi CM-3.C	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-3.D	Kontrol Perubahan Konfigurasi CM-3.D	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-3.D	Kontrol Perubahan Konfigurasi CM-3.D	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-3.e	Kontrol Perubahan Konfigurasi CM-3.E	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-3.e	Kontrol Perubahan Konfigurasi CM-3.E	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-3.f	Kontrol Perubahan Konfigurasi CM-3F	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-3.f	Kontrol Perubahan Konfigurasi CM-3F	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-3.g	Kontrol Perubahan Konfigurasi CM-3.G	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-3.g	Kontrol Perubahan Konfigurasi CM-3.G	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	access-keys-rotated	Kredensi diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktifkan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediakan sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi, pengembalian, dan pendelegasian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensi yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	secretsmanager-rotation-enabled-check	Aturan ini memastikan AWS rahasia Secrets Manager mengaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan.
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	secretsmanager-scheduled-rotation-success-periksa	Aturan ini memastikan bahwa AWS rahasia Secrets Manager telah berhasil diputar sesuai dengan jadwal rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode di mana rahasia aktif, dan berpotensi mengurangi dampak bisnis jika dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (1)	CM-5 (1) Pembatasan Akses untuk Perubahan | Penegakan/Audit Akses Otomatis	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (5)	CM-5 (5) Pembatasan Akses untuk Perubahan | Batasi Produksi/Hak Istimewa Operasional	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (5)	CM-5 (5) Pembatasan Akses untuk Perubahan | Batasi Produksi/Hak Istimewa Operasional	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (5)	CM-5 (5) Pembatasan Akses untuk Perubahan | Batasi Produksi/Hak Istimewa Operasional	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (5)	CM-5 (5) Pembatasan Akses untuk Perubahan | Batasi Produksi/Hak Istimewa Operasional	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktifkan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediakan sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (5)	CM-5 (5) Pembatasan Akses untuk Perubahan | Batasi Produksi/Hak Istimewa Operasional	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
CCCS-FPBMM-CM-5 (5)	CM-5 (5) Pembatasan Akses untuk Perubahan | Batasi Produksi/Hak Istimewa Operasional	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (5)	CM-5 (5) Pembatasan Akses untuk Perubahan | Batasi Produksi/Hak Istimewa Operasional	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi, pengembalian, dan pendelegasian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-CM-5 (5)	CM-5 (5) Pembatasan Akses untuk Perubahan | Batasi Produksi/Hak Istimewa Operasional	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (5)	CM-5 (5) Pembatasan Akses untuk Perubahan | Batasi Produksi/Hak Istimewa Operasional	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (5)	CM-5 (5) Pembatasan Akses untuk Perubahan | Batasi Produksi/Hak Istimewa Operasional	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (5)	CM-5 (5) Pembatasan Akses untuk Perubahan | Batasi Produksi/Hak Istimewa Operasional	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (5)	CM-5 (5) Pembatasan Akses untuk Perubahan | Batasi Produksi/Hak Istimewa Operasional	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5 (5)	CM-5 (5) Pembatasan Akses untuk Perubahan | Batasi Produksi/Hak Istimewa Operasional	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensi yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5.A	Pembatasan Akses CM-5.A untuk Perubahan	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5.A	Pembatasan Akses CM-5.A untuk Perubahan	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5.A	Pembatasan Akses CM-5.A untuk Perubahan	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5.A	Pembatasan Akses CM-5.A untuk Perubahan	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5.A	Pembatasan Akses CM-5.A untuk Perubahan	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
CCCS-FPBMM-CM-5.A	Pembatasan Akses CM-5.A untuk Perubahan	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5.A	Pembatasan Akses CM-5.A untuk Perubahan	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-CM-5.A	Pembatasan Akses CM-5.A untuk Perubahan	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5.A	Pembatasan Akses CM-5.A untuk Perubahan	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5.A	Pembatasan Akses CM-5.A untuk Perubahan	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5.A	Pembatasan Akses CM-5.A untuk Perubahan	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5.A	Pembatasan Akses CM-5.A untuk Perubahan	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-5.A	Pembatasan Akses CM-5.A untuk Perubahan	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensi yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6 (1)	Pengaturan Konfigurasi CM-6 (1) | Manajemen Sentral Otomatis/Aplikasi/Verifikasi	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6 (1)	Pengaturan Konfigurasi CM-6 (1) | Manajemen Sentral Otomatis/Aplikasi/Verifikasi	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6 (1)	Pengaturan Konfigurasi CM-6 (1) | Manajemen Sentral Otomatis/Aplikasi/Verifikasi	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	access-keys-rotated	Kredensi diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensi yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.A	Pengaturan Konfigurasi CM-6.A	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	access-keys-rotated	Kredensi diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensi yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.b	Pengaturan Konfigurasi CM-6.B	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	access-keys-rotated	Kredensi diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensi yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.c	Pengaturan Konfigurasi CM-6.C	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	access-keys-rotated	Kredensi diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensi yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-6.d	Pengaturan Konfigurasi CM-6.D	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-7.A	CM-7.A Fungsionalitas Terkecil	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-7.A	CM-7.A Fungsionalitas Terkecil	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-7.b	CM-7.B Fungsionalitas Terkecil	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-7.b	CM-7.B Fungsionalitas Terkecil	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-8 (1)	CM-8 (1) Inventaris Komponen Sistem Informasi | Pembaruan Selama Instalasi/Penghapusan	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-8 (1)	CM-8 (1) Inventaris Komponen Sistem Informasi | Pembaruan Selama Instalasi/Penghapusan	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-8 (2)	CM-8 (2) Inventaris Komponen Sistem Informasi | Pemeliharaan Otomatis	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-8 (2)	CM-8 (2) Inventaris Komponen Sistem Informasi | Pemeliharaan Otomatis	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-8 (3)	CM-8 (3) Inventaris Komponen Sistem Informasi | Deteksi Komponen Tidak Sah Otomatis	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-8 (3)	CM-8 (3) Inventaris Komponen Sistem Informasi | Deteksi Komponen Tidak Sah Otomatis	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-8 (3)	CM-8 (3) Inventaris Komponen Sistem Informasi | Deteksi Komponen Tidak Sah Otomatis	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-8 (3)	CM-8 (3) Inventaris Komponen Sistem Informasi | Deteksi Komponen Tidak Sah Otomatis	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-8.A	Inventaris Komponen Sistem Informasi CM-8.A	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-8.A	Inventaris Komponen Sistem Informasi CM-8.A	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-8.b	Inventaris Komponen Sistem Informasi CM-8.B	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-8.b	Inventaris Komponen Sistem Informasi CM-8.B	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-8.c	Inventaris Komponen Sistem Informasi CM-8.C	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-8.c	Inventaris Komponen Sistem Informasi CM-8.C	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-8.D	Inventaris Komponen Sistem Informasi CM-8.D	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-8.D	Inventaris Komponen Sistem Informasi CM-8.D	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-8.E	Inventaris Komponen Sistem Informasi CM-8.E	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CM-8.E	Inventaris Komponen Sistem Informasi CM-8.E	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (5)	CP-2 (5) Rencana Kontinjensi | Lanjutkan Misi Esensial/Fungsi Bisnis	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (5)	CP-2 (5) Rencana Kontinjensi | Lanjutkan Misi Esensial/Fungsi Bisnis	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (5)	CP-2 (5) Rencana Kontinjensi | Lanjutkan Misi Esensial/Fungsi Bisnis	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CCCS-FPBMM-CP-2 (5)	CP-2 (5) Rencana Kontinjensi | Lanjutkan Misi Esensial/Fungsi Bisnis	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (5)	CP-2 (5) Rencana Kontinjensi | Lanjutkan Misi Esensial/Fungsi Bisnis	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (5)	CP-2 (5) Rencana Kontinjensi | Lanjutkan Misi Esensial/Fungsi Bisnis	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (5)	CP-2 (5) Rencana Kontinjensi | Lanjutkan Misi Esensial/Fungsi Bisnis	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (5)	CP-2 (5) Rencana Kontinjensi | Lanjutkan Misi Esensial/Fungsi Bisnis	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan cadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (5)	CP-2 (5) Rencana Kontinjensi | Lanjutkan Misi Esensial/Fungsi Bisnis	dynamodb-resources-protected-by-rencana cadangan	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (5)	CP-2 (5) Rencana Kontinjensi | Lanjutkan Misi Esensial/Fungsi Bisnis	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (5)	CP-2 (5) Rencana Kontinjensi | Lanjutkan Misi Esensial/Fungsi Bisnis	ebs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (5)	CP-2 (5) Rencana Kontinjensi | Lanjutkan Misi Esensial/Fungsi Bisnis	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (5)	CP-2 (5) Rencana Kontinjensi | Lanjutkan Misi Esensial/Fungsi Bisnis	efs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (5)	CP-2 (5) Rencana Kontinjensi | Lanjutkan Misi Esensial/Fungsi Bisnis	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (5)	CP-2 (5) Rencana Kontinjensi | Lanjutkan Misi Esensial/Fungsi Bisnis	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (5)	CP-2 (5) Rencana Kontinjensi | Lanjutkan Misi Esensial/Fungsi Bisnis	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (5)	CP-2 (5) Rencana Kontinjensi | Lanjutkan Misi Esensial/Fungsi Bisnis	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (5)	CP-2 (5) Rencana Kontinjensi | Lanjutkan Misi Esensial/Fungsi Bisnis	rds-cluster-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (5)	CP-2 (5) Rencana Kontinjensi | Lanjutkan Misi Esensial/Fungsi Bisnis	rds-cluster-multi-az-diaktifkan	Cluster Amazon Relational Database Service (Amazon RDS) harus mengaktif kan replikasi Multi-AZ untuk membantu ketersediaan data yang disimpan. Setiap Availability Zone berjalan pada infrastru ktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutk an operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (5)	CP-2 (5) Rencana Kontinjensi | Lanjutkan Misi Esensial/Fungsi Bisnis	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (5)	CP-2 (5) Rencana Kontinjensi | Lanjutkan Misi Esensial/Fungsi Bisnis	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (5)	CP-2 (5) Rencana Kontinjensi | Lanjutkan Misi Esensial/Fungsi Bisnis	rds-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Relational Database Service (Amazon RDS) Anda merupakan AWS bagian dari paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (5)	CP-2 (5) Rencana Kontinjensi | Lanjutkan Misi Esensial/Fungsi Bisnis	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (5)	CP-2 (5) Rencana Kontinjensi | Lanjutkan Misi Esensial/Fungsi Bisnis	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (5)	CP-2 (5) Rencana Kontinjensi | Lanjutkan Misi Esensial/Fungsi Bisnis	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (5)	CP-2 (5) Rencana Kontinjensi | Lanjutkan Misi Esensial/Fungsi Bisnis	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (6)	CP-2 (6) Rencana Kontinjensi | Situs Pemrosesan/Penyimpanan Alternatif	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (6)	CP-2 (6) Rencana Kontinjensi | Situs Pemrosesan/Penyimpanan Alternatif	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (6)	CP-2 (6) Rencana Kontinjensi | Situs Pemrosesan/Penyimpanan Alternatif	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (6)	CP-2 (6) Rencana Kontinjensi | Situs Pemrosesan/Penyimpanan Alternatif	rds-cluster-multi-az-diaktifkan	Cluster Amazon Relational Database Service (Amazon RDS) harus mengaktifkan replikasi Multi-AZ untuk membantu ketersediaan data yang disimpan. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (6)	CP-2 (6) Rencana Kontinjensi | Situs Pemrosesan/Penyimpanan Alternatif	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2 (6)	CP-2 (6) Rencana Kontinjensi | Situs Pemrosesan/Penyimpanan Alternatif	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.A	Rencana Kontinjensi CP-2.A	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.A	Rencana Kontinjensi CP-2.A	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.A	Rencana Kontinjensi CP-2.A	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.A	Rencana Kontinjensi CP-2.A	rds-cluster-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.A	Rencana Kontinjensi CP-2.A	rds-cluster-multi-az-diaktifkan	Cluster Amazon Relational Database Service (Amazon RDS) harus mengaktifkan replikasi Multi-AZ untuk membantu ketersediaan data yang disimpan. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.A	Rencana Kontinjensi CP-2.A	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.A	Rencana Kontinjensi CP-2.A	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.A	Rencana Kontinjensi CP-2.A	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.b	Rencana Kontinjensi CP-2.B	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.b	Rencana Kontinjensi CP-2.B	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.b	Rencana Kontinjensi CP-2.B	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.b	Rencana Kontinjensi CP-2.B	rds-cluster-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.b	Rencana Kontinjensi CP-2.B	rds-cluster-multi-az-diaktifkan	Cluster Amazon Relational Database Service (Amazon RDS) harus mengaktifkan replikasi Multi-AZ untuk membantu ketersediaan data yang disimpan. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.b	Rencana Kontinjensi CP-2.B	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.b	Rencana Kontinjensi CP-2.B	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.b	Rencana Kontinjensi CP-2.B	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.c	Rencana Kontinjensi CP-2.C	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.c	Rencana Kontinjensi CP-2.C	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.c	Rencana Kontinjensi CP-2.C	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.c	Rencana Kontinjensi CP-2.C	rds-cluster-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.c	Rencana Kontinjensi CP-2.C	rds-cluster-multi-az-diaktifkan	Cluster Amazon Relational Database Service (Amazon RDS) harus mengaktif kan replikasi Multi-AZ untuk membantu ketersediaan data yang disimpan. Setiap Availability Zone berjalan pada infrastru ktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutk an operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.c	Rencana Kontinjensi CP-2.C	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.c	Rencana Kontinjensi CP-2.C	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.c	Rencana Kontinjensi CP-2.C	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.D	Rencana Kontinjensi CP-2.D	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.D	Rencana Kontinjensi CP-2.D	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.D	Rencana Kontinjensi CP-2.D	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.D	Rencana Kontinjensi CP-2.D	rds-cluster-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.D	Rencana Kontinjensi CP-2.D	rds-cluster-multi-az-diaktifkan	Cluster Amazon Relational Database Service (Amazon RDS) harus mengaktifkan replikasi Multi-AZ untuk membantu ketersediaan data yang disimpan. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.D	Rencana Kontinjensi CP-2.D	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.D	Rencana Kontinjensi CP-2.D	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.D	Rencana Kontinjensi CP-2.D	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.e	Rencana Kontinjensi CP-2.E	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.e	Rencana Kontinjensi CP-2.E	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.e	Rencana Kontinjensi CP-2.E	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.e	Rencana Kontinjensi CP-2.E	rds-cluster-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.e	Rencana Kontinjensi CP-2.E	rds-cluster-multi-az-diaktifkan	Cluster Amazon Relational Database Service (Amazon RDS) harus mengaktif kan replikasi Multi-AZ untuk membantu ketersediaan data yang disimpan. Setiap Availability Zone berjalan pada infrastru ktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutk an operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.e	Rencana Kontinjensi CP-2.E	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.e	Rencana Kontinjensi CP-2.E	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.e	Rencana Kontinjensi CP-2.E	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.f	Rencana Kontinjensi CP-2.F	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.f	Rencana Kontinjensi CP-2.F	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.f	Rencana Kontinjensi CP-2.F	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.f	Rencana Kontinjensi CP-2.F	rds-cluster-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.f	Rencana Kontinjensi CP-2.F	rds-cluster-multi-az-diaktifkan	Cluster Amazon Relational Database Service (Amazon RDS) harus mengaktif kan replikasi Multi-AZ untuk membantu ketersediaan data yang disimpan. Setiap Availability Zone berjalan pada infrastru ktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutk an operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.f	Rencana Kontinjensi CP-2.F	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.f	Rencana Kontinjensi CP-2.F	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.f	Rencana Kontinjensi CP-2.F	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.g	Rencana Kontinjensi CP-2.G	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.g	Rencana Kontinjensi CP-2.G	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.g	Rencana Kontinjensi CP-2.G	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.g	Rencana Kontinjensi CP-2.G	rds-cluster-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.g	Rencana Kontinjensi CP-2.G	rds-cluster-multi-az-diaktifkan	Cluster Amazon Relational Database Service (Amazon RDS) harus mengaktifkan replikasi Multi-AZ untuk membantu ketersediaan data yang disimpan. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.g	Rencana Kontinjensi CP-2.G	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.g	Rencana Kontinjensi CP-2.G	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-2.g	Rencana Kontinjensi CP-2.G	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (1)	CP-6 (1) Situs Penyimpanan Alternatif | Pemisahan dari Situs Utama	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (1)	CP-6 (1) Situs Penyimpanan Alternatif | Pemisahan dari Situs Utama	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (1)	CP-6 (1) Situs Penyimpanan Alternatif | Pemisahan dari Situs Utama	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CCCS-FPBMM-CP-6 (1)	CP-6 (1) Situs Penyimpanan Alternatif | Pemisahan dari Situs Utama	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (1)	CP-6 (1) Situs Penyimpanan Alternatif | Pemisahan dari Situs Utama	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (1)	CP-6 (1) Situs Penyimpanan Alternatif | Pemisahan dari Situs Utama	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (1)	CP-6 (1) Situs Penyimpanan Alternatif | Pemisahan dari Situs Utama	dynamodb-resources-protected-by-rencana cadangan	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (1)	CP-6 (1) Situs Penyimpanan Alternatif | Pemisahan dari Situs Utama	ebs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (1)	CP-6 (1) Situs Penyimpanan Alternatif | Pemisahan dari Situs Utama	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (1)	CP-6 (1) Situs Penyimpanan Alternatif | Pemisahan dari Situs Utama	efs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (1)	CP-6 (1) Situs Penyimpanan Alternatif | Pemisahan dari Situs Utama	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (1)	CP-6 (1) Situs Penyimpanan Alternatif | Pemisahan dari Situs Utama	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (1)	CP-6 (1) Situs Penyimpanan Alternatif | Pemisahan dari Situs Utama	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (1)	CP-6 (1) Situs Penyimpanan Alternatif | Pemisahan dari Situs Utama	rds-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Relational Database Service (Amazon RDS) Anda merupakan AWS bagian dari paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (1)	CP-6 (1) Situs Penyimpanan Alternatif | Pemisahan dari Situs Utama	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (1)	CP-6 (1) Situs Penyimpanan Alternatif | Pemisahan dari Situs Utama	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (1)	CP-6 (1) Situs Penyimpanan Alternatif | Pemisahan dari Situs Utama	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (2)	CP-6 (2) Situs Penyimpanan Alternatif | Waktu Pemulihan/Tujuan Titik	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (2)	CP-6 (2) Situs Penyimpanan Alternatif | Waktu Pemulihan/Tujuan Titik	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (2)	CP-6 (2) Situs Penyimpanan Alternatif | Waktu Pemulihan/Tujuan Titik	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CCCS-FPBMM-CP-6 (2)	CP-6 (2) Situs Penyimpanan Alternatif | Waktu Pemulihan/Tujuan Titik	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (2)	CP-6 (2) Situs Penyimpanan Alternatif | Waktu Pemulihan/Tujuan Titik	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (2)	CP-6 (2) Situs Penyimpanan Alternatif | Waktu Pemulihan/Tujuan Titik	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (2)	CP-6 (2) Situs Penyimpanan Alternatif | Waktu Pemulihan/Tujuan Titik	dynamodb-resources-protected-by-rencana cadangan	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (2)	CP-6 (2) Situs Penyimpanan Alternatif | Waktu Pemulihan/Tujuan Titik	ebs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (2)	CP-6 (2) Situs Penyimpanan Alternatif | Waktu Pemulihan/Tujuan Titik	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (2)	CP-6 (2) Situs Penyimpanan Alternatif | Waktu Pemulihan/Tujuan Titik	efs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (2)	CP-6 (2) Situs Penyimpanan Alternatif | Waktu Pemulihan/Tujuan Titik	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (2)	CP-6 (2) Situs Penyimpanan Alternatif | Waktu Pemulihan/Tujuan Titik	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (2)	CP-6 (2) Situs Penyimpanan Alternatif | Waktu Pemulihan/Tujuan Titik	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (2)	CP-6 (2) Situs Penyimpanan Alternatif | Waktu Pemulihan/Tujuan Titik	rds-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Relational Database Service (Amazon RDS) Anda merupakan AWS bagian dari paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (2)	CP-6 (2) Situs Penyimpanan Alternatif | Waktu Pemulihan/Tujuan Titik	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (2)	CP-6 (2) Situs Penyimpanan Alternatif | Waktu Pemulihan/Tujuan Titik	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6 (2)	CP-6 (2) Situs Penyimpanan Alternatif | Waktu Pemulihan/Tujuan Titik	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.A	CP-6.A Situs Penyimpanan Alternatif	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.A	CP-6.A Situs Penyimpanan Alternatif	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.A	CP-6.A Situs Penyimpanan Alternatif	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CCCS-FPBMM-CP-6.A	CP-6.A Situs Penyimpanan Alternatif	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.A	CP-6.A Situs Penyimpanan Alternatif	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.A	CP-6.A Situs Penyimpanan Alternatif	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.A	CP-6.A Situs Penyimpanan Alternatif	dynamodb-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.A	CP-6.A Situs Penyimpanan Alternatif	ebs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.A	CP-6.A Situs Penyimpanan Alternatif	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.A	CP-6.A Situs Penyimpanan Alternatif	efs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.A	CP-6.A Situs Penyimpanan Alternatif	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.A	CP-6.A Situs Penyimpanan Alternatif	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.A	CP-6.A Situs Penyimpanan Alternatif	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.A	CP-6.A Situs Penyimpanan Alternatif	rds-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Relational Database Service (Amazon RDS) Anda merupakan AWS bagian dari paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.A	CP-6.A Situs Penyimpanan Alternatif	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.A	CP-6.A Situs Penyimpanan Alternatif	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.A	CP-6.A Situs Penyimpanan Alternatif	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.B	Situs Penyimpanan Alternatif CP-6.B	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.B	Situs Penyimpanan Alternatif CP-6.B	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.B	Situs Penyimpanan Alternatif CP-6.B	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CCCS-FPBMM-CP-6.B	Situs Penyimpanan Alternatif CP-6.B	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.B	Situs Penyimpanan Alternatif CP-6.B	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.B	Situs Penyimpanan Alternatif CP-6.B	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.B	Situs Penyimpanan Alternatif CP-6.B	dynamodb-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.B	Situs Penyimpanan Alternatif CP-6.B	ebs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.B	Situs Penyimpanan Alternatif CP-6.B	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.B	Situs Penyimpanan Alternatif CP-6.B	efs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.B	Situs Penyimpanan Alternatif CP-6.B	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.B	Situs Penyimpanan Alternatif CP-6.B	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.B	Situs Penyimpanan Alternatif CP-6.B	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.B	Situs Penyimpanan Alternatif CP-6.B	rds-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Relational Database Service (Amazon RDS) Anda merupakan AWS bagian dari paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.B	Situs Penyimpanan Alternatif CP-6.B	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk cluster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.B	Situs Penyimpanan Alternatif CP-6.B	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-6.B	Situs Penyimpanan Alternatif CP-6.B	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9 (3)	CP-9 (3) Cadangan Sistem Informasi | Penyimpanan Terpisah untuk Informasi Kritis	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9 (3)	CP-9 (3) Cadangan Sistem Informasi | Penyimpanan Terpisah untuk Informasi Kritis	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9 (3)	CP-9 (3) Cadangan Sistem Informasi | Penyimpanan Terpisah untuk Informasi Kritis	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9 (3)	CP-9 (3) Cadangan Sistem Informasi | Penyimpanan Terpisah untuk Informasi Kritis	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9 (3)	CP-9 (3) Cadangan Sistem Informasi | Penyimpanan Terpisah untuk Informasi Kritis	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan cadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9 (3)	CP-9 (3) Cadangan Sistem Informasi | Penyimpanan Terpisah untuk Informasi Kritis	dynamodb-resources-protected-by-rencana cadangan	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9 (3)	CP-9 (3) Cadangan Sistem Informasi | Penyimpanan Terpisah untuk Informasi Kritis	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9 (3)	CP-9 (3) Cadangan Sistem Informasi | Penyimpanan Terpisah untuk Informasi Kritis	ebs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9 (3)	CP-9 (3) Cadangan Sistem Informasi | Penyimpanan Terpisah untuk Informasi Kritis	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9 (3)	CP-9 (3) Cadangan Sistem Informasi | Penyimpanan Terpisah untuk Informasi Kritis	efs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9 (3)	CP-9 (3) Cadangan Sistem Informasi | Penyimpanan Terpisah untuk Informasi Kritis	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9 (3)	CP-9 (3) Cadangan Sistem Informasi | Penyimpanan Terpisah untuk Informasi Kritis	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9 (3)	CP-9 (3) Cadangan Sistem Informasi | Penyimpanan Terpisah untuk Informasi Kritis	rds-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Relational Database Service (Amazon RDS) Anda merupakan AWS bagian dari paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9 (3)	CP-9 (3) Cadangan Sistem Informasi | Penyimpanan Terpisah untuk Informasi Kritis	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk cluster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9 (3)	CP-9 (3) Cadangan Sistem Informasi | Penyimpanan Terpisah untuk Informasi Kritis	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9 (3)	CP-9 (3) Cadangan Sistem Informasi | Penyimpanan Terpisah untuk Informasi Kritis	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9 (7)	CP-9 (7) Cadangan Sistem Informasi | Otorisasi Ganda	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9 (7)	CP-9 (7) Cadangan Sistem Informasi | Otorisasi Ganda	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.A	Cadangan Sistem Informasi CP-9.A	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.A	Cadangan Sistem Informasi CP-9.A	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.A	Cadangan Sistem Informasi CP-9.A	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CCCS-FPBMM-CP-9.A	Cadangan Sistem Informasi CP-9.A	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.A	Cadangan Sistem Informasi CP-9.A	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.A	Cadangan Sistem Informasi CP-9.A	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.A	Cadangan Sistem Informasi CP-9.A	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan cadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.A	Cadangan Sistem Informasi CP-9.A	dynamodb-resources-protected-by-rencana cadangan	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.A	Cadangan Sistem Informasi CP-9.A	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.A	Cadangan Sistem Informasi CP-9.A	ebs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
CCCS-FPBMM-CP-9.A	Cadangan Sistem Informasi CP-9.A	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.A	Cadangan Sistem Informasi CP-9.A	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.A	Cadangan Sistem Informasi CP-9.A	efs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.A	Cadangan Sistem Informasi CP-9.A	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.A	Cadangan Sistem Informasi CP-9.A	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.A	Cadangan Sistem Informasi CP-9.A	rds-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Relational Database Service (Amazon RDS) Anda merupakan AWS bagian dari paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.A	Cadangan Sistem Informasi CP-9.A	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-CP-9.A	Cadangan Sistem Informasi CP-9.A	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.A	Cadangan Sistem Informasi CP-9.A	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk cluster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.A	Cadangan Sistem Informasi CP-9.A	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.A	Cadangan Sistem Informasi CP-9.A	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.A	Cadangan Sistem Informasi CP-9.A	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.AA	Cadangan Sistem Informasi CP-9.AA	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.AA	Cadangan Sistem Informasi CP-9.AA	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.AA	Cadangan Sistem Informasi CP-9.AA	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CCCS-FPBMM-CP-9.AA	Cadangan Sistem Informasi CP-9.AA	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.AA	Cadangan Sistem Informasi CP-9.AA	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.AA	Cadangan Sistem Informasi CP-9.AA	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.AA	Cadangan Sistem Informasi CP-9.AA	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.AA	Cadangan Sistem Informasi CP-9.AA	dynamodb-resources-protected-by-rencana cadangan	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.AA	Cadangan Sistem Informasi CP-9.AA	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.AA	Cadangan Sistem Informasi CP-9.AA	ebs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
CCCS-FPBMM-CP-9.AA	Cadangan Sistem Informasi CP-9.AA	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.AA	Cadangan Sistem Informasi CP-9.AA	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.AA	Cadangan Sistem Informasi CP-9.AA	efs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.AA	Cadangan Sistem Informasi CP-9.AA	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.AA	Cadangan Sistem Informasi CP-9.AA	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.AA	Cadangan Sistem Informasi CP-9.AA	rds-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Relational Database Service (Amazon RDS) Anda merupakan AWS bagian dari paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.AA	Cadangan Sistem Informasi CP-9.AA	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-CP-9.AA	Cadangan Sistem Informasi CP-9.AA	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.AA	Cadangan Sistem Informasi CP-9.AA	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk cluster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.AA	Cadangan Sistem Informasi CP-9.AA	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.AA	Cadangan Sistem Informasi CP-9.AA	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.AA	Cadangan Sistem Informasi CP-9.AA	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.b	Cadangan Sistem Informasi CP-9.B	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.b	Cadangan Sistem Informasi CP-9.B	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.b	Cadangan Sistem Informasi CP-9.B	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CCCS-FPBMM-CP-9.b	Cadangan Sistem Informasi CP-9.B	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.b	Cadangan Sistem Informasi CP-9.B	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.b	Cadangan Sistem Informasi CP-9.B	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.b	Cadangan Sistem Informasi CP-9.B	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.b	Cadangan Sistem Informasi CP-9.B	dynamodb-resources-protected-by-rencana cadangan	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.b	Cadangan Sistem Informasi CP-9.B	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.b	Cadangan Sistem Informasi CP-9.B	ebs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
CCCS-FPBMM-CP-9.b	Cadangan Sistem Informasi CP-9.B	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.b	Cadangan Sistem Informasi CP-9.B	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.b	Cadangan Sistem Informasi CP-9.B	efs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.b	Cadangan Sistem Informasi CP-9.B	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.b	Cadangan Sistem Informasi CP-9.B	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.b	Cadangan Sistem Informasi CP-9.B	rds-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Relational Database Service (Amazon RDS) Anda merupakan AWS bagian dari paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.b	Cadangan Sistem Informasi CP-9.B	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-CP-9.b	Cadangan Sistem Informasi CP-9.B	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.b	Cadangan Sistem Informasi CP-9.B	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk cluster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.b	Cadangan Sistem Informasi CP-9.B	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.b	Cadangan Sistem Informasi CP-9.B	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.b	Cadangan Sistem Informasi CP-9.B	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.c	Cadangan Sistem Informasi CP-9.C	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.c	Cadangan Sistem Informasi CP-9.C	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.c	Cadangan Sistem Informasi CP-9.C	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CCCS-FPBMM-CP-9.c	Cadangan Sistem Informasi CP-9.C	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.c	Cadangan Sistem Informasi CP-9.C	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.c	Cadangan Sistem Informasi CP-9.C	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.c	Cadangan Sistem Informasi CP-9.C	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.c	Cadangan Sistem Informasi CP-9.C	dynamodb-resources-protected-by-rencana cadangan	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.c	Cadangan Sistem Informasi CP-9.C	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.c	Cadangan Sistem Informasi CP-9.C	ebs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
CCCS-FPBMM-CP-9.c	Cadangan Sistem Informasi CP-9.C	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.c	Cadangan Sistem Informasi CP-9.C	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.c	Cadangan Sistem Informasi CP-9.C	efs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.c	Cadangan Sistem Informasi CP-9.C	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.c	Cadangan Sistem Informasi CP-9.C	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.c	Cadangan Sistem Informasi CP-9.C	rds-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Relational Database Service (Amazon RDS) Anda merupakan AWS bagian dari paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.c	Cadangan Sistem Informasi CP-9.C	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-CP-9.c	Cadangan Sistem Informasi CP-9.C	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.c	Cadangan Sistem Informasi CP-9.C	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk cluster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.c	Cadangan Sistem Informasi CP-9.C	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.c	Cadangan Sistem Informasi CP-9.C	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.c	Cadangan Sistem Informasi CP-9.C	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.d	Cadangan Sistem Informasi CP-9.D	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.d	Cadangan Sistem Informasi CP-9.D	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.d	Cadangan Sistem Informasi CP-9.D	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CCCS-FPBMM-CP-9.d	Cadangan Sistem Informasi CP-9.D	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.d	Cadangan Sistem Informasi CP-9.D	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.d	Cadangan Sistem Informasi CP-9.D	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.d	Cadangan Sistem Informasi CP-9.D	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.d	Cadangan Sistem Informasi CP-9.D	dynamodb-resources-protected-by-rencana cadangan	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.d	Cadangan Sistem Informasi CP-9.D	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.d	Cadangan Sistem Informasi CP-9.D	ebs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
CCCS-FPBMM-CP-9.d	Cadangan Sistem Informasi CP-9.D	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.d	Cadangan Sistem Informasi CP-9.D	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.d	Cadangan Sistem Informasi CP-9.D	efs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.d	Cadangan Sistem Informasi CP-9.D	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.d	Cadangan Sistem Informasi CP-9.D	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.d	Cadangan Sistem Informasi CP-9.D	rds-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Relational Database Service (Amazon RDS) Anda merupakan AWS bagian dari paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.d	Cadangan Sistem Informasi CP-9.D	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-CP-9.d	Cadangan Sistem Informasi CP-9.D	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.d	Cadangan Sistem Informasi CP-9.D	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk cluster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.d	Cadangan Sistem Informasi CP-9.D	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.d	Cadangan Sistem Informasi CP-9.D	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-9.d	Cadangan Sistem Informasi CP-9.D	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-10.A	CP-10.A Pemulihan dan Rekonstitusi Sistem Informasi	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-10.A	CP-10.A Pemulihan dan Rekonstitusi Sistem Informasi	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-10.A	CP-10.A Pemulihan dan Rekonstitusi Sistem Informasi	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-10.A	CP-10.A Pemulihan dan Rekonstitusi Sistem Informasi	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-10.A	CP-10.A Pemulihan dan Rekonstitusi Sistem Informasi	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-10.A	CP-10.A Pemulihan dan Rekonstitusi Sistem Informasi	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-10.A	CP-10.A Pemulihan dan Rekonstitusi Sistem Informasi	rds-cluster-multi-az-diaktifkan	Cluster Amazon Relational Database Service (Amazon RDS) harus mengaktifkan replikasi Multi-AZ untuk membantu ketersediaan data yang disimpan. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-10.A	CP-10.A Pemulihan dan Rekonstitusi Sistem Informasi	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-10.A	CP-10.A Pemulihan dan Rekonstitusi Sistem Informasi	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk cluster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-10.A	CP-10.A Pemulihan dan Rekonstitusi Sistem Informasi	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-10.A	CP-10.A Pemulihan dan Rekonstitusi Sistem Informasi	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-CP-10.A	CP-10.A Pemulihan dan Rekonstitusi Sistem Informasi	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-2 (1)	IA-2 (1) Identifikasi dan Otentikasi (Pengguna Organisasi) | Akses Jaringan ke Akun Istimewa	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-2 (1)	IA-2 (1) Identifikasi dan Otentikasi (Pengguna Organisasi) | Akses Jaringan ke Akun Istimewa	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-2 (1)	IA-2 (1) Identifikasi dan Otentikasi (Pengguna Organisasi) | Akses Jaringan ke Akun Istimewa	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-2 (3)	IA-2 (3) Identifikasi dan Otentikasi (Pengguna Organisasi) | Akses Lokal ke Akun Istimewa	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-2 (3)	IA-2 (3) Identifikasi dan Otentikasi (Pengguna Organisasi) | Akses Lokal ke Akun Istimewa	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-2 (3)	IA-2 (3) Identifikasi dan Otentikasi (Pengguna Organisasi) | Akses Lokal ke Akun Istimewa	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-2 (8)	IA-2 (8) Identifikasi dan Otentikasi (Pengguna Organisasi) | Akses Jaringan ke Akun Istimewa - Replay Resistant	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-2 (8)	IA-2 (8) Identifikasi dan Otentikasi (Pengguna Organisasi) | Akses Jaringan ke Akun Istimewa - Replay Resistant	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-2 (8)	IA-2 (8) Identifikasi dan Otentikasi (Pengguna Organisasi) | Akses Jaringan ke Akun Istimewa - Replay Resistant	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-2 (11)	IA-2 (11) Identifikasi dan Otentikasi (Pengguna Organisasi) | Akses Jarak Jauh - Perangkat Terpisah	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-2 (11)	IA-2 (11) Identifikasi dan Otentikasi (Pengguna Organisasi) | Akses Jarak Jauh - Perangkat Terpisah	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-2 (11)	IA-2 (11) Identifikasi dan Otentikasi (Pengguna Organisasi) | Akses Jarak Jauh - Perangkat Terpisah	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-2.A	IA-2.A Identifikasi dan Otentikasi (Pengguna Organisasi)	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-2.A	IA-2.A Identifikasi dan Otentikasi (Pengguna Organisasi)	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-2.A	IA-2.A Identifikasi dan Otentikasi (Pengguna Organisasi)	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredensi masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-2.A	IA-2.A Identifikasi dan Otentikasi (Pengguna Organisasi)	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-4 (4)	IA-4 (4) Manajemen Pengidentifikasi | Identifikasi Status Pengguna	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-4.A	IA-4.A Manajemen Pengidentifikasi	access-keys-rotated	Kredensi diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-4.A	IA-4.A Manajemen Pengidentifikasi	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-4.A	IA-4.A Manajemen Pengidentifikasi	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-4.b	Manajemen Identifier IA-4.B	access-keys-rotated	Kredensi diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-4.b	Manajemen Identifier IA-4.B	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-4.b	Manajemen Identifier IA-4.B	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-4.c	Manajemen Identifier IA-4.C	access-keys-rotated	Kredensi diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-4.c	Manajemen Identifier IA-4.C	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-4.c	Manajemen Identifier IA-4.C	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-4.D	Manajemen Pengidentifikasi IA-4.D	access-keys-rotated	Kredensi diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-4.D	Manajemen Pengidentifikasi IA-4.D	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-4.D	Manajemen Pengidentifikasi IA-4.D	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-4.e	Manajemen Identifier IA-4.E	access-keys-rotated	Kredensi diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-4.e	Manajemen Identifier IA-4.E	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-4.e	Manajemen Identifier IA-4.E	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5 (1)	IA-5 (1) Manajemen Authenticator | Otentikasi Berbasis Kata Sandi	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5 (2)	IA-5 (2) Manajemen Authenticator | Otentikasi Berbasis PKI	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5 (2)	IA-5 (2) Manajemen Authenticator | Otentikasi Berbasis PKI	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5 (4)	IA-5 (4) Manajemen Authenticator | Dukungan Otomatis untuk Penentuan Kekuatan Kata Sandi	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5 (8)	IA-5 (8) Manajemen Authenticator | Beberapa Akun Sistem Informasi	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5 (8)	IA-5 (8) Manajemen Authenticator | Beberapa Akun Sistem Informasi	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5 (8)	IA-5 (8) Manajemen Authenticator | Beberapa Akun Sistem Informasi	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredensi masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.A	IA-5.A Manajemen Authenticator	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.A	IA-5.A Manajemen Authenticator	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.A	IA-5.A Manajemen Authenticator	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredensi masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.A	IA-5.A Manajemen Authenticator	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.b	IA-5.B Manajemen Authenticator	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.b	IA-5.B Manajemen Authenticator	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.b	IA-5.B Manajemen Authenticator	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredensi masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.b	IA-5.B Manajemen Authenticator	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.c	Manajemen Autentikator IA-5.C	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.c	Manajemen Autentikator IA-5.C	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.c	Manajemen Autentikator IA-5.C	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.c	Manajemen Autentikator IA-5.C	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.D	Manajemen Autentikator IA-5.D	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.D	Manajemen Autentikator IA-5.D	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.D	Manajemen Autentikator IA-5.D	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.D	Manajemen Autentikator IA-5.D	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.e	IA-5.E Manajemen Authenticator	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.e	IA-5.E Manajemen Authenticator	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.e	IA-5.E Manajemen Authenticator	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredensi masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.e	IA-5.E Manajemen Authenticator	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.f	IA-5.F Manajemen Authenticator	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.f	IA-5.F Manajemen Authenticator	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.f	IA-5.F Manajemen Authenticator	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredensi masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.f	IA-5.F Manajemen Authenticator	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.g	Manajemen Autentikator IA-5.G	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.g	Manajemen Autentikator IA-5.G	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.g	Manajemen Autentikator IA-5.G	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.g	Manajemen Autentikator IA-5.G	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.h	IA-5.H Manajemen Authenticator	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.h	IA-5.H Manajemen Authenticator	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.h	IA-5.H Manajemen Authenticator	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredensi masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.h	IA-5.H Manajemen Authenticator	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.i	IA-5.I Manajemen Authenticator	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.i	IA-5.I Manajemen Authenticator	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.i	IA-5.I Manajemen Authenticator	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredensi masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.i	IA-5.I Manajemen Authenticator	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.j	IA-5.J Manajemen Authenticator	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.j	IA-5.J Manajemen Authenticator	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.j	IA-5.J Manajemen Authenticator	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredensi masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IA-5.j	IA-5.J Manajemen Authenticator	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-IR-6 (1)	IR-6 (1) Pelaporan Insiden | Pelaporan Otomatis	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MA-3.A	MA-3.A Alat Pemeliharaan	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MA-3.A	MA-3.A Alat Pemeliharaan	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
CCCS-FPBMM-MA-4 (1)	MA-4 (1) Pemeliharaan Nonlokal | Audit dan Tinjauan	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MA-4 (1)	MA-4 (1) Pemeliharaan Nonlokal | Audit dan Tinjauan	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
CCCS-FPBMM-MA-4 (1)	MA-4 (1) Pemeliharaan Nonlokal | Audit dan Tinjauan	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MA-4 (1)	MA-4 (1) Pemeliharaan Nonlokal | Audit dan Tinjauan	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MA-4 (1)	MA-4 (1) Pemeliharaan Nonlokal | Audit dan Tinjauan	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MA-4 (1)	MA-4 (1) Pemeliharaan Nonlokal | Audit dan Tinjauan	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MA-4 (1)	MA-4 (1) Pemeliharaan Nonlokal | Audit dan Tinjauan	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MA-4 (1)	MA-4 (1) Pemeliharaan Nonlokal | Audit dan Tinjauan	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MA-4 (1)	MA-4 (1) Pemeliharaan Nonlokal | Audit dan Tinjauan	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MA-4 (1)	MA-4 (1) Pemeliharaan Nonlokal | Audit dan Tinjauan	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MA-4 (1)	MA-4 (1) Pemeliharaan Nonlokal | Audit dan Tinjauan	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-MP-2.A	MP-2.A Akses Media	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-RA-5.A	Pemindaian Kerentanan RA-5.A	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-RA-5.b	Pemindaian Kerentanan RA-5.B	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-RA-5.c	Pemindaian Kerentanan RA-5.C	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-RA-5.D	Pemindaian Kerentanan RA-5.D	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-RA-5.e	Pemindaian Kerentanan RA-5.E	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SA-10 (1)	SA-10 (1) Manajemen Konfigurasi Pengembang | Verifikasi Integritas Perangkat Lunak/Firmware	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-5.A	SC-5.A Penolakan Perlindungan Layanan	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-5.A	SC-5.A Penolakan Perlindungan Layanan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-6.A	SC-6.A Ketersediaan Sumber Daya	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-6.A	SC-6.A Ketersediaan Sumber Daya	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-6.A	SC-6.A Ketersediaan Sumber Daya	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-6.A	SC-6.A Ketersediaan Sumber Daya	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-SC-6.A	SC-6.A Ketersediaan Sumber Daya	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-6.A	SC-6.A Ketersediaan Sumber Daya	rds-cluster-multi-az-diaktifkan	Cluster Amazon Relational Database Service (Amazon RDS) harus mengaktifkan replikasi Multi-AZ untuk membantu ketersediaan data yang disimpan. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-6.A	SC-6.A Ketersediaan Sumber Daya	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-6.A	SC-6.A Ketersediaan Sumber Daya	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (3)	SC-7 (3) Perlindungan Batas | Titik Akses	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-SC-7 (3)	SC-7 (3) Perlindungan Batas | Titik Akses	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-SC-7 (3)	SC-7 (3) Perlindungan Batas | Titik Akses	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (3)	SC-7 (3) Perlindungan Batas | Titik Akses	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
CCCS-FPBMM-SC-7 (3)	SC-7 (3) Perlindungan Batas | Titik Akses	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (3)	SC-7 (3) Perlindungan Batas | Titik Akses	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (3)	SC-7 (3) Perlindungan Batas | Titik Akses	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
CCCS-FPBMM-SC-7 (3)	SC-7 (3) Perlindungan Batas | Titik Akses	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (3)	SC-7 (3) Perlindungan Batas | Titik Akses	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (3)	SC-7 (3) Perlindungan Batas | Titik Akses	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (3)	SC-7 (3) Perlindungan Batas | Titik Akses	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-SC-7 (3)	SC-7 (3) Perlindungan Batas | Titik Akses	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (3)	SC-7 (3) Perlindungan Batas | Titik Akses	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (3)	SC-7 (3) Perlindungan Batas | Titik Akses	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (3)	SC-7 (3) Perlindungan Batas | Titik Akses	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
CCCS-FPBMM-SC-7 (3)	SC-7 (3) Perlindungan Batas | Titik Akses	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (3)	SC-7 (3) Perlindungan Batas | Titik Akses	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
CCCS-FPBMM-SC-7 (3)	SC-7 (3) Perlindungan Batas | Titik Akses	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (3)	SC-7 (3) Perlindungan Batas | Titik Akses	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	elb-predefined-security-policy-ssl-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa pendengar SSL Classic Elastic Load Balancing Anda menggunakan kebijakan keamanan yang telah ditentukan sebelumnya. Elastic Load Balancing menyediakan konfigurasi negosiasi SSL yang telah ditentukan sebelumnya yang digunakan untuk negosiasi SSL ketika koneksi dibuat antara klien dan penyeimbang beban Anda. Konfigurasi negosiasi SSL memberikan kompatibilitas dengan berbagai klien dan menggunakan algoritma kriptografi berkekuatan tinggi. Aturan ini mengharuskan Anda menetapkan kebijakan keamanan yang telah ditentuka

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			n untuk pendengar SSL Anda. Kebijakan keamanan default adalah: ELBSecurity Policy-TLS-1-2-2017-0. Nilai aktual harus mencerminkan kebijakan organisasi Anda
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigurasi ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (4)	SC-7 (4) Perlindungan Batas | Layanan Telekomunikasi Eksternal	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (5)	SC-7 (5) Perlindungan Batas | Tolak secara Default/Izinkan dengan Pengecualian	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (5)	SC-7 (5) Perlindungan Batas | Tolak secara Default/Izinkan dengan Pengecualian	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (5)	SC-7 (5) Perlindungan Batas | Tolak secara Default/Izinkan dengan Pengecualian	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (5)	SC-7 (5) Perlindungan Batas | Tolak secara Default/Izinkan dengan Pengecualian	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (7)	SC-7 (7) Perlindungan Batas | Mencegah Terowongan Terpisah untuk Perangkat Jarak Jauh	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-SC-7 (7)	SC-7 (7) Perlindungan Batas | Mencegah Terowongan Terpisah untuk Perangkat Jarak Jauh	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-SC-7 (7)	SC-7 (7) Perlindungan Batas | Mencegah Terowongan Terpisah untuk Perangkat Jarak Jauh	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (7)	SC-7 (7) Perlindungan Batas | Mencegah Terowongan Terpisah untuk Perangkat Jarak Jauh	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-SC-7 (7)	SC-7 (7) Perlindungan Batas | Mencegah Terowongan Terpisah untuk Perangkat Jarak Jauh	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (7)	SC-7 (7) Perlindungan Batas | Mencegah Terowongan Terpisah untuk Perangkat Jarak Jauh	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
CCCS-FPBMM-SC-7 (7)	SC-7 (7) Perlindungan Batas | Mencegah Terowongan Terpisah untuk Perangkat Jarak Jauh	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (7)	SC-7 (7) Perlindungan Batas | Mencegah Terowongan Terpisah untuk Perangkat Jarak Jauh	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-SC-7 (7)	SC-7 (7) Perlindungan Batas | Mencegah Terowongan Terpisah untuk Perangkat Jarak Jauh	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (7)	SC-7 (7) Perlindungan Batas | Mencegah Terowongan Terpisah untuk Perangkat Jarak Jauh	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (7)	SC-7 (7) Perlindungan Batas | Mencegah Terowongan Terpisah untuk Perangkat Jarak Jauh	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (7)	SC-7 (7) Perlindungan Batas | Mencegah Terowongan Terpisah untuk Perangkat Jarak Jauh	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (7)	SC-7 (7) Perlindungan Batas | Mencegah Terowongan Terpisah untuk Perangkat Jarak Jauh	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
CCCS-FPBMM-SC-7 (7)	SC-7 (7) Perlindungan Batas | Mencegah Terowongan Terpisah untuk Perangkat Jarak Jauh	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (7)	SC-7 (7) Perlindungan Batas | Mencegah Terowongan Terpisah untuk Perangkat Jarak Jauh	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
CCCS-FPBMM-SC-7 (7)	SC-7 (7) Perlindungan Batas | Mencegah Terowongan Terpisah untuk Perangkat Jarak Jauh	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (7)	SC-7 (7) Perlindungan Batas | Mencegah Terowongan Terpisah untuk Perangkat Jarak Jauh	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7 (7)	SC-7 (7) Perlindungan Batas | Mencegah Terowongan Terpisah untuk Perangkat Jarak Jauh	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .
CCCS-FPBMM-SC-7.A	SC-7.A Perlindungan Batas	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.A	SC-7.A Perlindungan Batas	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-SC-7.A	SC-7.A Perlindungan Batas	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.A	SC-7.A Perlindungan Batas	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
CCCS-FPBMM-SC-7.A	SC-7.A Perlindungan Batas	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.A	SC-7.A Perlindungan Batas	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.A	SC-7.A Perlindungan Batas	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.A	SC-7.A Perlindungan Batas	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
CCCS-FPBMM-SC-7.A	SC-7.A Perlindungan Batas	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.A	SC-7.A Perlindungan Batas	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.A	SC-7.A Perlindungan Batas	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.A	SC-7.A Perlindungan Batas	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-SC-7.A	SC-7.A Perlindungan Batas	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.A	SC-7.A Perlindungan Batas	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.A	SC-7.A Perlindungan Batas	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.A	SC-7.A Perlindungan Batas	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.A	SC-7.A Perlindungan Batas	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
CCCS-FPBMM-SC-7.A	SC-7.A Perlindungan Batas	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.A	SC-7.A Perlindungan Batas	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
CCCS-FPBMM-SC-7.A	SC-7.A Perlindungan Batas	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.A	SC-7.A Perlindungan Batas	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.A	SC-7.A Perlindungan Batas	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.A	SC-7.A Perlindungan Batas	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.b	Perlindungan Batas SC-7.B	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-SC-7.b	Perlindungan Batas SC-7.B	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-SC-7.b	Perlindungan Batas SC-7.B	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.b	Perlindungan Batas SC-7.B	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
CCCS-FPBMM-SC-7.b	Perlindungan Batas SC-7.B	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.b	Perlindungan Batas SC-7.B	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.b	Perlindungan Batas SC-7.B	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.b	Perlindungan Batas SC-7.B	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
CCCS-FPBMM-SC-7.b	Perlindungan Batas SC-7.B	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.b	Perlindungan Batas SC-7.B	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.b	Perlindungan Batas SC-7.B	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.b	Perlindungan Batas SC-7.B	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-SC-7.b	Perlindungan Batas SC-7.B	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.b	Perlindungan Batas SC-7.B	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.b	Perlindungan Batas SC-7.B	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.b	Perlindungan Batas SC-7.B	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.b	Perlindungan Batas SC-7.B	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
CCCS-FPBMM-SC-7.b	Perlindungan Batas SC-7.B	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.b	Perlindungan Batas SC-7.B	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
CCCS-FPBMM-SC-7.b	Perlindungan Batas SC-7.B	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.b	Perlindungan Batas SC-7.B	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.b	Perlindungan Batas SC-7.B	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.b	Perlindungan Batas SC-7.B	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.c	Perlindungan Batas SC-7.C	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-SC-7.c	Perlindungan Batas SC-7.C	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-SC-7.c	Perlindungan Batas SC-7.C	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.c	Perlindungan Batas SC-7.C	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
CCCS-FPBMM-SC-7.c	Perlindungan Batas SC-7.C	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.c	Perlindungan Batas SC-7.C	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.c	Perlindungan Batas SC-7.C	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.c	Perlindungan Batas SC-7.C	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
CCCS-FPBMM-SC-7.c	Perlindungan Batas SC-7.C	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.c	Perlindungan Batas SC-7.C	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.c	Perlindungan Batas SC-7.C	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.c	Perlindungan Batas SC-7.C	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
CCCS-FPBMM-SC-7.c	Perlindungan Batas SC-7.C	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.c	Perlindungan Batas SC-7.C	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.c	Perlindungan Batas SC-7.C	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.c	Perlindungan Batas SC-7.C	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.c	Perlindungan Batas SC-7.C	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
CCCS-FPBMM-SC-7.c	Perlindungan Batas SC-7.C	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.c	Perlindungan Batas SC-7.C	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
CCCS-FPBMM-SC-7.c	Perlindungan Batas SC-7.C	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.c	Perlindungan Batas SC-7.C	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.c	Perlindungan Batas SC-7.C	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-7.c	Perlindungan Batas SC-7.C	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-8 (1)	SC-8 (1) Kerahasia an dan Integritas Transmisi | Perlindun gan Fisik Kriptografi atau Alternatif	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
CCCS-FPBMM-SC-8 (1)	SC-8 (1) Kerahasia an dan Integritas Transmisi | Perlindun gan Fisik Kriptografi atau Alternatif	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-8 (1)	SC-8 (1) Kerahasiaan dan Integritas Transmisi | Perlindungan Fisik Kriptografi atau Alternatif	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-8 (1)	SC-8 (1) Kerahasiaan dan Integritas Transmisi | Perlindungan Fisik Kriptografi atau Alternatif	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-8 (1)	SC-8 (1) Kerahasiaan dan Integritas Transmisi | Perlindungan Fisik Kriptografi atau Alternatif	elb-predefined-security-policy-ssl-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa pendengar SSL Classic Elastic Load Balancing Anda menggunakan kebijakan keamanan yang telah ditentukan sebelumnya. Elastic Load Balancing menyediakan konfigurasi negosiasi SSL yang telah ditentukan sebelumnya yang digunakan untuk negosiasi SSL ketika koneksi dibuat antara klien dan penyeimbang beban Anda. Konfigurasi negosiasi SSL memberikan kompatibilitas dengan berbagai klien dan menggunakan algoritma kriptografi berkekuatan tinggi. Aturan ini mengharuskan Anda menetapkan kebijakan keamanan yang telah ditentuka

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			n untuk pendengar SSL Anda. Kebijakan keamanan default adalah: ELBSecurity Policy-TLS-1-2-2017-0. Nilai aktual harus mencerminkan kebijakan organisasi Anda
CCCS-FPBMM-SC-8 (1)	SC-8 (1) Kerahasiaan dan Integritas Transmisi | Perlindungan Fisik Kriptografi atau Alternatif	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-8 (1)	SC-8 (1) Kerahasiaan dan Integritas Transmisi | Perlindungan Fisik Kriptografi atau Alternatif	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
CCCS-FPBMM-SC-8 (1)	SC-8 (1) Kerahasiaan dan Integritas Transmisi | Perlindungan Fisik Kriptografi atau Alternatif	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-8 (1)	SC-8 (1) Kerahasia an dan Integritas Transmisi | Perlindun gan Fisik Kriptografi atau Alternatif	s3- bucket-ssl-request s-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
CCCS-FPBMM-SC-8.A	SC-8.A Kerahasia an dan Integritas Transmisi	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-8.A	SC-8.A Kerahasiaan dan Integritas Transmisi	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.
CCCS-FPBMM-SC-8.A	SC-8.A Kerahasiaan dan Integritas Transmisi	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-8.A	SC-8.A Kerahasiaan dan Integritas Transmisi	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-8.A	SC-8.A Kerahasiaan dan Integritas Transmisi	elb-predefined-security-policy-ssl-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa pendengar SSL Classic Elastic Load Balancing Anda menggunakan kebijakan keamanan yang telah ditentukan sebelumnya. Elastic Load Balancing menyediakan konfigurasi negosiasi SSL yang telah ditentukan sebelumnya yang digunakan untuk negosiasi SSL ketika koneksi dibuat antara klien dan penyeimbang beban Anda. Konfigurasi negosiasi SSL memberikan kompatibilitas dengan berbagai klien dan menggunakan algoritma kriptografi berkekuatan tinggi. Aturan ini mengharuskan Anda menetapkan kebijakan keamanan yang telah ditentuka

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			n untuk pendengar SSL Anda. Kebijakan keamanan default adalah: ELBSecurity Policy-TLS-1-2-2017-0. Nilai aktual harus mencerminkan kebijakan organisasi Anda
CCCS-FPBMM-SC-8.A	SC-8.A Kerahasiaan dan Integritas Transmisi	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-8.A	SC-8.A Kerahasiaan dan Integritas Transmisi	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
CCCS-FPBMM-SC-8.A	SC-8.A Kerahasiaan dan Integritas Transmisi	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-8.A	SC-8.A Kerahasiaan dan Integritas Transmisi	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-12 (1)	SC-12 (1) Pembentukan dan Manajemen Kunci Kriptografi | Ketersediaan	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.
CCCS-FPBMM-SC-12 (2)	SC-12 (2) Pembentukan dan Manajemen Kunci Kriptografi | Kunci Simetris	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-12 (2)	SC-12 (2) Pembentukan dan Manajemen Kunci Kriptografi | Kunci Simetris	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.
CCCS-FPBMM-SC-12.A	SC-12.A Pembentukan dan Manajemen Kunci Kriptografi	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-12.A	SC-12.A Pembentukan dan Manajemen Kunci Kriptografi	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-13.A	SC-13.A Perlindungan Kriptografi	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
CCCS-FPBMM-SC-13.A	SC-13.A Perlindungan Kriptografi	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-13.A	SC-13.A Perlindungan Kriptografi	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrai l jejak Anda.
CCCS-FPBMM-SC-13.A	SC-13.A Perlindungan Kriptografi	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CCCS-FPBMM-SC-13.A	SC-13.A Perlindungan Kriptografi	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-13.A	SC-13.A Perlindungan Kriptografi	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
CCCS-FPBMM-SC-13.A	SC-13.A Perlindungan Kriptografi	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-13.A	SC-13.A Perlindungan Kriptografi	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-13.A	SC-13.A Perlindungan Kriptografi	elb-predefined-security-policy-ssl-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa pendengar SSL Classic Elastic Load Balancing Anda menggunakan kebijakan keamanan yang telah ditentukan sebelumnya. Elastic Load Balancing menyediakan konfigurasi negosiasi SSL yang telah ditentukan sebelumnya yang digunakan untuk negosiasi SSL ketika koneksi dibuat antara klien dan penyeimbang beban Anda. Konfigurasi negosiasi SSL memberikan kompatibilitas dengan berbagai klien dan menggunakan algoritma kriptografi berkekuatan tinggi. Aturan ini mengharuskan Anda menetapkan kebijakan keamanan yang telah ditentuka

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			n untuk pendengar SSL Anda. Kebijakan keamanan default adalah: ELBSecurity Policy-TLS-1-2-2017-0. Nilai aktual harus mencerminkan kebijakan organisasi Anda
CCCS-FPBMM-SC-13.A	SC-13.A Perlindungan Kriptografi	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
CCCS-FPBMM-SC-13.A	SC-13.A Perlindungan Kriptografi	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-13.A	SC-13.A Perlindungan Kriptografi	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
CCCS-FPBMM-SC-13.A	SC-13.A Perlindungan Kriptografi	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-13.A	SC-13.A Perlindungan Kriptografi	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CCCS-FPBMM-SC-13.A	SC-13.A Perlindungan Kriptografi	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-13.A	SC-13.A Perlindungan Kriptografi	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-13.A	SC-13.A Perlindungan Kriptografi	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CCCS-FPBMM-SC-13.A	SC-13.A Perlindungan Kriptografi	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-13.A	SC-13.A Perlindungan Kriptografi	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
CCCS-FPBMM-SC-13.A	SC-13.A Perlindungan Kriptografi	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-13.A	SC-13.A Perlindungan Kriptografi	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CCCS-FPBMM-SC-13.A	SC-13.A Perlindungan Kriptografi	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-13.A	SC-13.A Perlindungan Kriptografi	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-13.A	SC-13.A Perlindungan Kriptografi	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-22.A	SC-22.A Arsitektur dan Penyediaan untuk Layanan Resolusi Nama/Alamat	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
CCCS-FPBMM-SC-23.A	Keaslian Sesi SC-23.A	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-23.A	Keaslian Sesi SC-23.A	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
CCCS-FPBMM-SC-23.A	Keaslian Sesi SC-23.A	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-n ode enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkrip si memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-23.A	Keaslian Sesi SC-23.A	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-23.A	Keaslian Sesi SC-23.A	elb-predefined-security-policy-ssl-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa pendengar SSL Classic Elastic Load Balancing Anda menggunakan kebijakan keamanan yang telah ditentukan sebelumnya. Elastic Load Balancing menyediakan konfigurasi negosiasi SSL yang telah ditentukan sebelumnya yang digunakan untuk negosiasi SSL ketika koneksi dibuat antara klien dan penyeimbang beban Anda. Konfigurasi negosiasi SSL memberikan kompatibilitas dengan berbagai klien dan menggunakan algoritma kriptografi berkekuatan tinggi. Aturan ini mengharuskan Anda menetapkan kebijakan keamanan yang telah ditentuka

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			n untuk pendengar SSL Anda. Kebijakan keamanan default adalah: ELBSecurity Policy-TLS-1-2-2017-0. Nilai aktual harus mencerminkan kebijakan organisasi Anda
CCCS-FPBMM-SC-23.A	Keaslian Sesi SC-23.A	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-23.A	Keaslian Sesi SC-23.A	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
CCCS-FPBMM-SC-23.A	Keaslian Sesi SC-23.A	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-23.A	Keaslian Sesi SC-23.A	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
CCCS-FPBMM-SC-28 (1)	SC-28 (1) Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-28 (1)	SC-28 (1) Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CCCS-FPBMM-SC-28 (1)	SC-28 (1) Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
CCCS-FPBMM-SC-28 (1)	SC-28 (1) Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-28 (1)	SC-28 (1) Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
CCCS-FPBMM-SC-28 (1)	SC-28 (1) Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
CCCS-FPBMM-SC-28 (1)	SC-28 (1) Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-28 (1)	SC-28 (1) Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-28 (1)	SC-28 (1) Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-28 (1)	SC-28 (1) Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CCCS-FPBMM-SC-28 (1)	SC-28 (1) Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-28 (1)	SC-28 (1) Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CCCS-FPBMM-SC-28 (1)	SC-28 (1) Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-28 (1)	SC-28 (1) Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-28 (1)	SC-28 (1) Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CCCS-FPBMM-SC-28.A	SC-28.A Perlindungan Informasi saat Istirahat	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-28.A	SC-28.A Perlindungan Informasi saat Istirahat	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
CCCS-FPBMM-SC-28.A	SC-28.A Perlindungan Informasi saat Istirahat	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CCCS-FPBMM-SC-28.A	SC-28.A Perlindungan Informasi saat Istirahat	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-28.A	SC-28.A Perlindungan Informasi saat Istirahat	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
CCCS-FPBMM-SC-28.A	SC-28.A Perlindungan Informasi saat Istirahat	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-28.A	SC-28.A Perlindungan Informasi saat Istirahat	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-28.A	SC-28.A Perlindungan Informasi saat Istirahat	elb-predefined-security-policy-ssl-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa pendengar SSL Classic Elastic Load Balancing Anda menggunakan kebijakan keamanan yang telah ditentukan sebelumnya. Elastic Load Balancing menyediakan konfigurasi negosiasi SSL yang telah ditentukan sebelumnya yang digunakan untuk negosiasi SSL ketika koneksi dibuat antara klien dan penyeimbang beban Anda. Konfigurasi negosiasi SSL memberikan kompatibilitas dengan berbagai klien dan menggunakan algoritma kriptografi berkekuatan tinggi. Aturan ini mengharuskan Anda menetapkan kebijakan keamanan yang telah ditentuka

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			n untuk pendengar SSL Anda. Kebijakan keamanan default adalah: ELBSecurity Policy-TLS-1-2-2017-0. Nilai aktual harus mencerminkan kebijakan organisasi Anda
CCCS-FPBMM-SC-28.A	SC-28.A Perlindungan Informasi saat Istirahat	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
CCCS-FPBMM-SC-28.A	SC-28.A Perlindungan Informasi saat Istirahat	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-28.A	SC-28.A Perlindungan Informasi saat Istirahat	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
CCCS-FPBMM-SC-28.A	SC-28.A Perlindungan Informasi saat Istirahat	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-28.A	SC-28.A Perlindungan Informasi saat Istirahat	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CCCS-FPBMM-SC-28.A	SC-28.A Perlindungan Informasi saat Istirahat	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-28.A	SC-28.A Perlindungan Informasi saat Istirahat	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-28.A	SC-28.A Perlindungan Informasi saat Istirahat	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CCCS-FPBMM-SC-28.A	SC-28.A Perlindungan Informasi saat Istirahat	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-28.A	SC-28.A Perlindungan Informasi saat Istirahat	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
CCCS-FPBMM-SC-28.A	SC-28.A Perlindungan Informasi saat Istirahat	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-28.A	SC-28.A Perlindungan Informasi saat Istirahat	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CCCS-FPBMM-SC-28.A	SC-28.A Perlindungan Informasi saat Istirahat	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-28.A	SC-28.A Perlindungan Informasi saat Istirahat	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SC-28.A	SC-28.A Perlindungan Informasi saat Istirahat	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2 (2)	SI-2 (2) Remediasi Cacat | Status Remediasi Cacat Otomatis	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2 (2)	SI-2 (2) Remediasi Cacat | Status Remediasi Cacat Otomatis	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2 (2)	SI-2 (2) Remediasi Cacat | Status Remediasi Cacat Otomatis	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2 (2)	SI-2 (2) Remediasi Cacat | Status Remediasi Cacat Otomatis	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-SI-2 (2)	SI-2 (2) Remediasi Cacat | Status Remediasi Cacat Otomatis	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2 (2)	SI-2 (2) Remediasi Cacat | Status Remediasi Cacat Otomatis	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2 (2)	SI-2 (2) Remediasi Cacat | Status Remediasi Cacat Otomatis	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2 (2)	SI-2 (2) Remediasi Cacat | Status Remediasi Cacat Otomatis	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
CCCS-FPBMM-SI-2 (2)	SI-2 (2) Remediasi Cacat | Status Remediasi Cacat Otomatis	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2 (2)	SI-2 (2) Remediasi Cacat | Status Remediasi Cacat Otomatis	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2 (2)	SI-2 (2) Remediasi Cacat | Status Remediasi Cacat Otomatis	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2 (2)	SI-2 (2) Remediasi Cacat | Status Remediasi Cacat Otomatis	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2 (3)	SI-2 (3) Remediasi Cacat | Saatnya Remediasi Kelemahan/Tolok Ukur untuk Tindakan Korektif	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.A	SI-2.A Remediasi Cacat	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.A	SI-2.A Remediasi Cacat	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.A	SI-2.A Remediasi Cacat	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.A	SI-2.A Remediasi Cacat	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-SI-2.A	SI-2.A Remediasi Cacat	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.A	SI-2.A Remediasi Cacat	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.A	SI-2.A Remediasi Cacat	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.A	SI-2.A Remediasi Cacat	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
CCCS-FPBMM-SI-2.A	SI-2.A Remediasi Cacat	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.A	SI-2.A Remediasi Cacat	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.A	SI-2.A Remediasi Cacat	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.A	SI-2.A Remediasi Cacat	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.b	Remediasi Cacat SI-2.B	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.b	Remediasi Cacat SI-2.B	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.b	Remediasi Cacat SI-2.B	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.b	Remediasi Cacat SI-2.B	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-SI-2.b	Remediasi Cacat SI-2.B	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.b	Remediasi Cacat SI-2.B	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.b	Remediasi Cacat SI-2.B	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.b	Remediasi Cacat SI-2.B	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
CCCS-FPBMM-SI-2.b	Remediasi Cacat SI-2.B	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.b	Remediasi Cacat SI-2.B	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.b	Remediasi Cacat SI-2.B	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.b	Remediasi Cacat SI-2.B	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.c	Remediasi Cacat SI-2.C	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.c	Remediasi Cacat SI-2.C	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.c	Remediasi Cacat SI-2.C	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.c	Remediasi Cacat SI-2.C	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-SI-2.c	Remediasi Cacat SI-2.C	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.c	Remediasi Cacat SI-2.C	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.c	Remediasi Cacat SI-2.C	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.c	Remediasi Cacat SI-2.C	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
CCCS-FPBMM-SI-2.c	Remediasi Cacat SI-2.C	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.c	Remediasi Cacat SI-2.C	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.c	Remediasi Cacat SI-2.C	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.c	Remediasi Cacat SI-2.C	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.D	Remediasi Cacat SI-2.D	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.D	Remediasi Cacat SI-2.D	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.D	Remediasi Cacat SI-2.D	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.D	Remediasi Cacat SI-2.D	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
CCCS-FPBMM-SI-2.D	Remediasi Cacat SI-2.D	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.D	Remediasi Cacat SI-2.D	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.D	Remediasi Cacat SI-2.D	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.D	Remediasi Cacat SI-2.D	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
CCCS-FPBMM-SI-2.D	Remediasi Cacat SI-2.D	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.D	Remediasi Cacat SI-2.D	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.D	Remediasi Cacat SI-2.D	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-2.D	Remediasi Cacat SI-2.D	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-3 (1)	SI-3 (1) Perlindungan Kode Berbahaya | Manajemen Pusat	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-3 (7)	SI-3 (7) Perlindungan Kode Berbahaya | Deteksi Berbasis Non Tanda Tangan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-3.A	SI-3.A Perlindungan Kode Berbahaya	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-3.A	SI-3.A Perlindungan Kode Berbahaya	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-3.A	SI-3.A Perlindungan Kode Berbahaya	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-3.A	SI-3.A Perlindungan Kode Berbahaya	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-3.A	SI-3.A Perlindungan Kode Berbahaya	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-3.b	SI-3.B Perlindungan Kode Berbahaya	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-3.b	SI-3.B Perlindungan Kode Berbahaya	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-3.b	SI-3.B Perlindungan Kode Berbahaya	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-3.b	SI-3.B Perlindungan Kode Berbahaya	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-3.c	SI-3.C Perlindungan Kode Berbahaya	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-3.c	SI-3.C Perlindungan Kode Berbahaya	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-3.c	SI-3.C Perlindungan Kode Berbahaya	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-3.c	SI-3.C Perlindungan Kode Berbahaya	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-3.D	SI-3.D Perlindungan Kode Berbahaya	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-3.D	SI-3.D Perlindungan Kode Berbahaya	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-3.D	SI-3.D Perlindungan Kode Berbahaya	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-3.D	SI-3.D Perlindungan Kode Berbahaya	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4 (1)	SI-4 (1) Pemantauan Sistem Informasi | Sistem Deteksi Intrusi Seluruh Sistem	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4 (1)	SI-4 (1) Pemantauan Sistem Informasi | Sistem Deteksi Intrusi Seluruh Sistem	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4 (2)	SI-4 (2) Pemantauan Sistem Informasi | Alat Otomatis untuk Analisis Real-Time	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4 (2)	SI-4 (2) Pemantauan Sistem Informasi | Alat Otomatis untuk Analisis Real-Time	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4 (4)	SI-4 (4) Pemantauan Sistem Informasi | Lalu Lintas Komunikasi Masuk dan Keluar	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4 (4)	SI-4 (4) Pemantauan Sistem Informasi | Lalu Lintas Komunikasi Masuk dan Keluar	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4 (5)	SI-4 (5) Pemantauan Sistem Informasi | Peringatan yang Dihasilkan Sistem	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4 (11)	SI-4 (11) Pemantauan Sistem Informasi | Menganalisis Anomali Lalu Lintas Komunikasi	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4 (11)	SI-4 (11) Pemantauan Sistem Informasi | Menganalisis Anomali Lalu Lintas Komunikasi	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4 (16)	SI-4 (16) Pemantauan Sistem Informasi | Informasi Pemantauan Berkorelasi	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4 (16)	SI-4 (16) Pemantauan Sistem Informasi | Informasi Pemantauan Berkorelasi	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4 (20)	SI-4 (20) Pemantauan Sistem Informasi | Privileged User	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4 (23)	SI-4 (23) Pemantauan Sistem Informasi | Perangkat Berbasis Host	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4 (23)	SI-4 (23) Pemantauan Sistem Informasi | Perangkat Berbasis Host	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4.A	SI-4.A Pemantauan Sistem Informasi	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4.A	SI-4.A Pemantauan Sistem Informasi	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4.A	SI-4.A Pemantauan Sistem Informasi	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
CCCS-FPBMM-SI-4.A	SI-4.A Pemantauan Sistem Informasi	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4.A	SI-4.A Pemantauan Sistem Informasi	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4.b	Pemantauan Sistem Informasi SI-4.B	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4.b	Pemantauan Sistem Informasi SI-4.B	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4.b	Pemantauan Sistem Informasi SI-4.B	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
CCCS-FPBMM-SI-4.b	Pemantauan Sistem Informasi SI-4.B	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4.b	Pemantauan Sistem Informasi SI-4.B	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4.c	Pemantauan Sistem Informasi SI-4.C	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4.c	Pemantauan Sistem Informasi SI-4.C	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4.c	Pemantauan Sistem Informasi SI-4.C	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
CCCS-FPBMM-SI-4.c	Pemantauan Sistem Informasi SI-4.C	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4.c	Pemantauan Sistem Informasi SI-4.C	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4.D	Pemantauan Sistem Informasi SI-4.D	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4.D	Pemantauan Sistem Informasi SI-4.D	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4.D	Pemantauan Sistem Informasi SI-4.D	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
CCCS-FPBMM-SI-4.D	Pemantauan Sistem Informasi SI-4.D	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4.D	Pemantauan Sistem Informasi SI-4.D	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4.e	Pemantauan Sistem Informasi SI-4.E	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4.e	Pemantauan Sistem Informasi SI-4.E	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4.e	Pemantauan Sistem Informasi SI-4.E	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
CCCS-FPBMM-SI-4.e	Pemantauan Sistem Informasi SI-4.E	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4.e	Pemantauan Sistem Informasi SI-4.E	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4.f	Pemantauan Sistem Informasi SI-4.F	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4.f	Pemantauan Sistem Informasi SI-4.F	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4.f	Pemantauan Sistem Informasi SI-4.F	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
CCCS-FPBMM-SI-4.f	Pemantauan Sistem Informasi SI-4.F	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4.f	Pemantauan Sistem Informasi SI-4.F	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4.g	Pemantauan Sistem Informasi SI-4.G	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4.g	Pemantauan Sistem Informasi SI-4.G	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4.g	Pemantauan Sistem Informasi SI-4.G	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
CCCS-FPBMM-SI-4.g	Pemantauan Sistem Informasi SI-4.G	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-4.g	Pemantauan Sistem Informasi SI-4.G	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-5.A	SI-5.A Peringatan Keamanan, Penasihat , dan Arahan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-5.b	SI-5.B Peringatan Keamanan, Penasihat , dan Arahan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-5.c	SI-5.C Peringatan Keamanan, Penasihat , dan Arahan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCC-FPBMM-SI-5.D	SI-5.D Peringatan Keamanan, Penasihat , dan Arahan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-7 (1)	SI-7 (1) Perangkat Lunak, Firmware, dan Integritas Informasi | Pemeriksaan Integrita s	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-7 (7)	SI-7 (7) Perangkat Lunak, Firmware, dan Integritas Informasi | Integrasi Deteksi dan Respon	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-7.A	SI-7.A Perangkat Lunak, Firmware, dan Integritas Informasi	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CCCS-FPBMM-SI-12.A	SI-12.A Penanganan dan Retensi Informasi	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

Templat

Template ini tersedia di GitHub: Praktik Terbaik Operasional untuk Canadian Centre for Cyber Security (CCCS) Medium Cloud Control Profile.

Praktik Terbaik Operasional untuk Tolok Ukur AWS Yayasan CIS v1.4 Level 1

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini menyediakan contoh pemetaan antara Center for Internet Security (CIS) Amazon Web Services Foundation v1.4 Level 1 dan aturan AWS Config terkelola/ Pemeriksaan Proses.AWS Config Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau

beberapa kontrol CIS Amazon Web Services Foundation v1.4 Level 1. Kontrol CIS Amazon Web Services Foundation v1.4 Level 1 dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

Untuk informasi selengkapnya tentang pemeriksaan proses, lihat pemeriksaan proses.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.1	Pertahankan detail kontak saat ini	account-contact-details-configured (pemeriksaan proses)	Pastikan email kontak dan nomor telepon untuk AWS akun terkini dan petakan ke lebih dari satu orang di organisasi Anda. Di bagian Akun Saya di konsol, pastikan informasi yang benar ditentukan di bagian Informasi Kontak. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundatio ns Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/
1.2	Pastikan informasi kontak keamanan terdaftar	account-security-c ontact-configured (Pemeriksaan Proses)	Pastikan email kontak dan nomor telepon untuk tim keamanan organisasi Anda terkini. Di bagian Akun Saya di Konsol

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			AWS Manajemen, pastikan informasi yang benar ditentukan di bagian Keamanan. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundatio ns Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/
1.4	Pastikan tidak ada kunci akses pengguna 'root'	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.5	Pastikan MFA diaktifkan untuk pengguna 'root'	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.7	Hilangkan penggunaan pengguna 'root' untuk tugas administratif dan harian	root-account-regular-use (Pemeriksaan Proses)	Pastikan penggunaan akun root dihindari untuk tugas sehari-hari. Dalam IAM, jalankan laporan kredensyal untuk memeriksa kapan pengguna root terakhir digunakan. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundations Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.8	Pastikan kebijakan kata sandi IAM membutuhkan panjang minimum 14 atau lebih	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.9	Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.10	Pastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna yang memiliki kata sandi konsol	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensyal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.11	Jangan mengatur kunci akses selama penyiapan pengguna awal untuk semua pengguna yang memiliki kata sandi konsol	iam-user-console-and- api-access-at-creation (Pemeriksaan Proses)	Pastikan kunci akses tidak diatur selama penyiapan pengguna awal untuk semua pengguna yang memiliki kata sandi konsol. Untuk semua pengguna dengan akses konsol, bandingkan 'Waktu pembuatan ` pengguna dengan tanggal `Created` Kunci Akses. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundations Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.12	Pastikan kredensil yang tidak digunakan selama 45 hari atau lebih dinonaktifkan	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (nilai Standar CIS: 45). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.13	Pastikan hanya ada satu kunci akses aktif yang tersedia untuk setiap pengguna tunggal	iam-user-single-access-key (Pemeriksaan Proses)	Pastikan hanya ada satu kunci akses aktif yang tersedia untuk setiap pengguna tunggal. Untuk semua pengguna, periksa bahwa hanya ada satu kunci aktif yang digunakan dalam tab Security Credentials untuk setiap pengguna dalam IAM. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundations Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.14	Pastikan kunci akses diputar setiap 90 hari atau kurang	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.15	Pastikan Pengguna Menerima Izin Hanya Melalui Grup	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.15	Pastikan Pengguna Menerima Izin Hanya Melalui Grup	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.15	Pastikan Pengguna Menerima Izin Hanya Melalui Grup	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.16	Pastikan kebijakan IAM yang memungkinkan hak administratif “*: *” penuh tidak dilampirkan	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.17	Pastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Support	iam-policy-in-use	AWS Identity and Access Managemen t (IAM) dapat membantu Anda mengelola izin akses dan otorisasi dengan memastika n bahwa kebijakan IAM ditetapkan ke pengguna, peran, atau grup yang sesuai. Membatasi kebijakan ini juga mencakup prinsip-p rinsip hak istimewa yang paling rendah dan pemisahan tugas. Aturan ini mengharus kan Anda menyetel PolicYarn ke arn:aws:i am: AWSSuppor t :aws:policy/ Access, untuk manajemen insiden dengan Support. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.19	Pastikan bahwa semua sertifikat SSL/TLS kedaluwarsa yang disimpan di IAM dihapus AWS	iam-expired-certificates (Pemeriksaan Proses)	Pastikan bahwa semua sertifikat SSL/TLS kedaluwarsa yang disimpan di IAM dihapus. Dari baris perintah dengan AWS CLI yang diinstal jalankan perintah 'AWS iam list-server-certificates' dan tentukan apakah ada sertifikat server yang kedaluwarsa. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundations Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.20	Pastikan AWS IAM Access Analyzer diaktifkan	iam-access-analyzer-enabled (Pemeriksaan Proses)	Pastikan IAM Access Analyzer diaktifkan. Di bagian IAM konsol, pilih Access Analyzer dan pastikan STATUS diatur ke Aktif. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundations Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.1.3	Pastikan MFA Delete diaktifkan pada bucket S3	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Menambahkan penghapusan otentikasi multi faktor (MFA) ke bucket S3 memerlukan faktor otentikasi tambahan untuk mengubah status versi bucket Anda atau untuk menghapus dan versi objek. MFA delete dapat menambahk an lapisan keamanan tambahan jika kredensyal keamanan dikompromikan atau akses tidak sah diberikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.1.5	Pastikan Bucket S3 dikonfigurasi dengan 'Blokir akses publik (pengaturan bucket) '	s3- account-level-publ ic-access -blok-per iodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.1.5	Pastikan Bucket S3 dikonfigurasi dengan 'Blokir akses publik (pengaturan bucket) '	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
2.2.1	Pastikan enkripsi volume EBS diaktifkan	volume terenkripsi	Karena data senstif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.1	Pastikan enkripsi volume EBS diaktifkan	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
2.3.1	Pastikan enkripsi diaktifkan untuk Instans RDS	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.3.1	Pastikan enkripsi diaktifkan untuk Instans RDS	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1	Pastikan CloudTrail diaktifkan di semua wilayah	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
3.3	Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
3.4	Pastikan CloudTrail jalur terintegrasi dengan Log CloudWatch	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6	Pastikan pencatata n akses bucket S3 diaktifkan pada bucket CloudTrail S3	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediak an metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinc i untuk permintaa n yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Pastikan filter metrik log dan alarm ada untuk panggilan API yang tidak sah	alarm-unauthorized-api-calls (Pemeriksaan Proses)	Pastikan filter metrik log dan alarm ada untuk panggilan API yang tidak sah. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundations Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/
4.2	Pastikan ada filter metrik log dan alarm untuk login Management Console tanpa MFA	alarm-sign-in-without-mfa (Pemeriksaan Proses)	Pastikan filter metrik log dan alarm ada untuk login AWS Management Console tanpa Multi-Factor Authentication (MFA). Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundations Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.3	Pastikan filter metrik log dan alarm ada untuk penggunaan akun 'root'	alarm-root-account-use (Pemeriksaan Proses)	Pastikan filter metrik log dan alarm ada untuk penggunaan akun root. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundations Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/
4.4	Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM	alarm-iam-policy-change (Pemeriksaan Proses)	Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundations Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.5	Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail konfigurasi	alarm-cloudtrail-config-change (Pemeriksaan Proses)	Pastikan filter metrik log dan alarm ada untuk perubahan AWS CloudTrail konfigurasi. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundatio ns Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/
4.8	Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3	alarm-s3- bucket-policy-change (Pemeriksaan Proses)	Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket Amazon S3. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundatio ns Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.12	Pastikan filter metrik log dan alarm ada untuk perubahan gateway jaringan	alarm-vpc-network-gateway-perubahan (Pemeriksaan Proses)	Pastikan filter metrik log dan alarm ada untuk perubahan gateway jaringan. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundatio ns Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/
4.13	Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute	alarm-vpc-route-table-perubahan (Pemeriksaan Proses)	Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundatio ns Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.14	Pastikan filter metrik log dan alarm ada untuk perubahan VPC	alarm-vpc-change (Pemeriksaan Proses)	Pastikan filter metrik log dan alarm ada untuk perubahan Amazon Virtual Private Cloud (VPC). Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundatio ns Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/
4.15	Pastikan filter metrik log dan alarm ada untuk perubahan AWS Organizations	alarm-organizations-change (Pemeriksaan Proses)	Pastikan filter metrik log dan alarm ada untuk perubahan AWS Organizations. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundatio ns Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.1	Pastikan tidak ada Jaringan yang ACLs mengizink an masuknya dari 0.0.0.0/0 ke port administrasi server jarak jauh	nacl-no-unrestricted-ssh-rdp	Pastikan tidak ada jaringan yang ACLs memungkinkan masuknya publik ke port administrasi server jarak jauh. Dalam bagian VPC konsol, pastikan ada jaringan ACLs dengan sumber '0.0.0.0/0' dengan memungkinkan port atau rentang port termasuk port admin server jarak jauh. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundatio ns Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.2	Pastikan tidak ada grup keamanan yang mengizink an masuknya dari 0.0.0.0/0 ke port administrasi server jarak jauh	dibatasi ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.2	Pastikan tidak ada grup keamanan yang mengizink an masuknya dari 0.0.0.0/0 ke port administrasi server jarak jauh	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Nilai standar CIS: 3389). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

Templat

Template ini tersedia di GitHub: Praktik Terbaik Operasional untuk Tolok Ukur AWS Yayasan CIS v1.4 Level 1.

Praktik Terbaik Operasional untuk Tolok Ukur AWS Yayasan CIS v1.4 Level 2

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini menyediakan contoh pemetaan antara Center for Internet Security (CIS) Amazon Web Services Foundation v1.4 Level 2 dan aturan AWS Config terkelola/ Pemeriksaan Proses.AWS Config Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau beberapa kontrol CIS Amazon Web Services Foundation v1.4 Level 2. Kontrol CIS Amazon Web Services Foundation v1.4 Level 2 dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

Untuk informasi selengkapnya tentang pemeriksaan proses, lihat pemeriksaan proses.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.1	Pertahankan detail kontak saat ini	account-contact-details-configured (pemeriksaan proses)	Pastikan email kontak dan nomor telepon untuk AWS akun terkini dan petakan ke lebih dari satu orang di organisasi Anda. Di bagian Akun Saya di konsol, pastikan informasi yang benar ditentukan di bagian Informasi Kontak. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			CIS Amazon Web Services Foundatio ns Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/
1.2	Pastikan informasi kontak keamanan terdaftar	account-security-contact-configured (Pemeriksaan Proses)	Pastikan email kontak dan nomor telepon untuk tim keamanan organisasi Anda terkini. Di bagian Akun Saya di Konsol AWS Manajemen, pastikan informasi yang benar ditentukan di bagian Keamanan. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundatio ns Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4	Pastikan tidak ada kunci akses pengguna 'root'	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.5	Pastikan MFA diaktifkan untuk pengguna 'root'	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.6	Pastikan MFA perangkat keras diaktifkan untuk akun pengguna 'root'	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.7	Hilangkan penggunaan pengguna 'root' untuk tugas administratif dan harian	root-account-regular-use (Pemeriksaan Proses)	Pastikan penggunaan akun root dihindari untuk tugas sehari-hari. Dalam IAM, jalankan laporan kredensyal untuk memeriksa kapan pengguna root terakhir digunakan. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundations Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.8	Pastikan kebijakan kata sandi IAM membutuhkan panjang minimum 14 atau lebih	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.9	Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.10	Pastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna yang memiliki kata sandi konsol	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.11	Jangan mengatur kunci akses selama penyiapan pengguna awal untuk semua pengguna yang memiliki kata sandi konsol	iam-user-console-a nd- api-access-at-crea tion (Pemeriksaan Proses)	Pastikan kunci akses tidak diatur selama penyiapan pengguna awal untuk semua pengguna yang memiliki kata sandi konsol. Untuk semua pengguna dengan akses konsol, bandingkan 'Waktu pembuatan ` pengguna dengan tanggal `Created` Kunci Akses. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundatio ns Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity. org/benchmark/amaz on_web_layanan/

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.12	Pastikan kredensil yang tidak digunakan selama 45 hari atau lebih dinonaktifkan	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsageUsia (nilai Standar CIS: 45). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.13	Pastikan hanya ada satu kunci akses aktif yang tersedia untuk setiap pengguna	iam-user-single-access-key (Pemeriksaan Proses)	Pastikan hanya ada satu kunci akses aktif yang tersedia untuk setiap pengguna tunggal. Untuk semua pengguna, periksa bahwa hanya ada satu kunci aktif yang digunakan dalam tab Security Credentials untuk setiap pengguna dalam IAM. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundations Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.14	Pastikan kunci akses diputar setiap 90 hari atau kurang	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.15	Pastikan Pengguna Menerima Izin Hanya Melalui Grup	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.15	Pastikan Pengguna Menerima Izin Hanya Melalui Grup	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.15	Pastikan Pengguna Menerima Izin Hanya Melalui Grup	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.16	Pastikan kebijakan IAM yang memungkinkan hak administratif “*: *” penuh tidak dilampirkan	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.17	Pastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Support	iam-policy-in-use	AWS Identity and Access Managemen t (IAM) dapat membantu Anda mengelola izin akses dan otorisasi dengan memastika n bahwa kebijakan IAM ditetapkan ke pengguna, peran, atau grup yang sesuai. Membatasi kebijakan ini juga mencakup prinsip-p rinsip hak istimewa yang paling rendah dan pemisahan tugas. Aturan ini mengharus kan Anda menyetel PolicYarn ke arn:aws:i am: AWSSuppor t :aws:policy/ Access, untuk manajemen insiden dengan Support. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.18	Pastikan peran instans IAM digunakan untuk akses AWS sumber daya dari instance	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.
1.19	Pastikan bahwa semua sertifikat SSL/TLS kedaluwarsa yang disimpan di IAM dihapus AWS	iam-expired-certificates (Pemeriksaan Proses)	Pastikan bahwa semua sertifikat SSL/TLS kedaluwarsa yang disimpan di IAM dihapus. Dari baris perintah dengan AWS CLI yang diinstal jalankan perintah 'AWS iam list-server-certificates' dan tentukan apakah ada sertifikat server yang kedaluwarsa. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundations Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.20	Pastikan AWS IAM Access Analyzer diaktifkan	iam-access-analyzer-enabled (Pemeriksaan Proses)	Pastikan IAM Access Analyzer diaktifkan. Di bagian IAM konsol, pilih Access Analyzer dan pastikan STATUS diatur ke Aktif. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundations Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/
1.21	Pastikan pengguna dikelola secara terpusat dari federasi identitas atau AWS Organizations untuk lingkungan multi-akun	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.1.1	Pastikan semua bucket S3 digunakan encryption-at-rest	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
2.1.2	Pastikan Kebijakan Bucket S3 disetel untuk menolak permintaan HTTP	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.1.3	Pastikan MFA Delete diaktifkan pada bucket S3	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Menambahkan penghapusan otentikasi multi faktor (MFA) ke bucket S3 memerlukan faktor otentikasi tambahan untuk mengubah status versi bucket Anda atau untuk menghapus dan versi objek. MFA delete dapat menambahk an lapisan keamanan tambahan jika kredensi keamanan dikompromikan atau akses tidak sah diberikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.1.5	Pastikan Bucket S3 dikonfigurasi dengan 'Blokir akses publik (pengaturan bucket) '	s3- account-level-publ ic-access -blok-per iodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.1.5	Pastikan Bucket S3 dikonfigurasi dengan 'Blokir akses publik (pengaturan bucket) '	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
2.2.1	Pastikan enkripsi volume EBS diaktifkan	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.1	Pastikan enkripsi volume EBS diaktifkan	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
2.3.1	Pastikan enkripsi diaktifkan untuk Instans RDS	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.3.1	Pastikan enkripsi diaktifkan untuk Instans RDS	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1	Pastikan CloudTrail diaktifkan di semua wilayah	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.2	Pastikan validasi file CloudTrail log diaktifkan	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
3.3	Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
3.4	Pastikan CloudTrail jalur terintegrasi dengan Log CloudWatch	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5	Pastikan AWS Config diaktifkan di semua wilayah	config-enabled-all-regions (Pemeriksaan Proses)	Pastikan AWS Config diaktifkan di semua AWS Wilayah. Di bagian AWS Config konsol, untuk setiap Wilayah yang diaktifkan, pastikan perekam AWS Config dikonfigurasi dengan benar. Pastikan pencatatan AWS sumber daya global diaktifkan setidakny a di satu Wilayah. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundatio ns Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity. org/benchmark/amaz on_web_layanan/

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6	Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.7	Pastikan CloudTrail log dienkripsi saat istirahat menggunakan KMS CMKs	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
3.8	Pastikan rotasi untuk pelanggan yang CMKs dibuat diaktifkan	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.
3.9	Pastikan pencatatan aliran VPC diaktifkan di semua VPCs	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.10	Pastikan bahwa pencatatan tingkat Objek untuk peristiwa penulisan diaktifkan untuk bucket S3	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
3.11	Pastikan pencatatan tingkat Objek untuk peristiwa baca diaktifkan untuk bucket S3	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Pastikan filter metrik log dan alarm ada untuk panggilan API yang tidak sah	alarm-unauthorized-api-calls (Pemeriksaan Proses)	Pastikan filter metrik log dan alarm ada untuk panggilan API yang tidak sah. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundations Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/
4.2	Pastikan ada filter metrik log dan alarm untuk login Management Console tanpa MFA	alarm-sign-in-without-mfa (Pemeriksaan Proses)	Pastikan filter metrik log dan alarm ada untuk login AWS Management Console tanpa Multi-Factor Authentication (MFA). Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundations Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.3	Pastikan filter metrik log dan alarm ada untuk penggunaan akun 'root'	alarm-root-account-use (Pemeriksaan Proses)	Pastikan filter metrik log dan alarm ada untuk penggunaan akun root. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundations Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/
4.4	Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM	alarm-iam-policy-change (Pemeriksaan Proses)	Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundations Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4,5	Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail konfigurasi	alarm-cloudtrail-config-change (Pemeriksaan Proses)	Pastikan filter metrik log dan alarm ada untuk perubahan AWS CloudTrail konfigurasi. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundations Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/
4.6	Pastikan ada filter metrik log dan alarm untuk kegagalan autentikasi AWS Management Console	alarm-console-auth-failures (Pemeriksaan Proses)	Pastikan filter metrik log dan alarm ada untuk kegagalan autentikasi AWS Management Console. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundations Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.7	Pastikan filter metrik log dan alarm ada untuk menonakti fkan atau terjadwal penghapusan pelanggan yang dibuat CMKs	alarm-kms-disable-or-delete-cmk (Pemeriksaan Proses)	Pastikan filter metrik log dan alarm ada untuk menonakti fkan atau terjadwal penghapusan pelanggan yang dibuat. CMKs Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundations Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.8	Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3	alarm-s3- bucket-policy-change (Pemeriksaan Proses)	Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket Amazon S3. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundations Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/
4.9	Pastikan filter metrik log dan alarm ada untuk perubahan AWS konfigurasi Config	alarm-aws-config-change (Pemeriksaan Proses)	Pastikan filter metrik log dan alarm ada untuk perubahan AWS konfigurasi Config. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundations Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.10	Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan	alarm-vpc-secrity-group-perubahan (Pemeriksaan Proses)	Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundatio ns Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/
4.11	Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)	alarm-vpc-nacl-change (Pemeriksaan Proses)	Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL). Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundatio ns Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.12	Pastikan filter metrik log dan alarm ada untuk perubahan gateway jaringan	alarm-vpc-network-gateway-perubahan (Pemeriksaan Proses)	Pastikan filter metrik log dan alarm ada untuk perubahan gateway jaringan. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundatio ns Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/
4.13	Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute	alarm-vpc-route-table-perubahan (Pemeriksaan Proses)	Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundatio ns Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.14	Pastikan filter metrik log dan alarm ada untuk perubahan VPC	alarm-vpc-change (Pemeriksaan Proses)	Pastikan filter metrik log dan alarm ada untuk perubahan Amazon Virtual Private Cloud (VPC). Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundatio ns Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/
4.15	Pastikan filter metrik log dan alarm ada untuk perubahan AWS Organizations	alarm-organizations-change (Pemeriksaan Proses)	Pastikan filter metrik log dan alarm ada untuk perubahan AWS Organizations. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundatio ns Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.1	Pastikan tidak ada Jaringan yang ACLs mengizink an masuknya dari 0.0.0.0/0 ke port administrasi server jarak jauh	nacl-no-unrestricted-ssh-rdp	Pastikan tidak ada jaringan yang ACLs memungkinkan masuknya publik ke port administrasi server jarak jauh. Dalam bagian VPC konsol, pastikan ada jaringan ACLs dengan sumber '0.0.0.0/0' dengan memungkinkan port atau rentang port termasuk port admin server jarak jauh. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundatio ns Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amaz on_web_layanan/

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.2	Pastikan tidak ada grup keamanan yang mengizink an masuknya dari 0.0.0.0/0 ke port administrasi server jarak jauh	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.2	Pastikan tidak ada grup keamanan yang mengizink an masuknya dari 0.0.0.0/0 ke port administrasi server jarak jauh	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Nilai standar CIS: 3389). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.3	Pastikan grup keamanan default dari setiap VPC membatasi semua lalu lintas	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.4	Pastikan tabel perutean untuk peering VPC adalah “akses paling sedikit”	vpc-peering-least-access (Pemeriksaan Proses)	Pastikan tabel perutean untuk peering VPC Amazon adalah “akses paling sedikit”. Di bagian VPC konsol, periksa entri tabel rute untuk memastikan bahwa jumlah subnet atau host paling sedikit diperluka n untuk mencapai tujuan peering dapat dirutekan. Untuk detail lebih lanjut tentang audit kontrol ini, silakan merujuk ke dokumen CIS Amazon Web Services Foundatio ns Benchmark versi 1.4.0 yang tersedia di https://www.cisecurity.org/benchmark/amazon_web_layanan/

Templat

Template ini tersedia di GitHub: Praktik Terbaik Operasional untuk Tolok Ukur AWS Yayasan CIS v1.4 Level 2.

Praktik Terbaik Operasional untuk Kontrol Keamanan Kritis CIS v8 IG1

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan

biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini menyediakan contoh pemetaan antara Center for Internet Security (CIS) Critical Security Controls v8 dan aturan AWS Config IG1 terkelola. Masing-masing AWS Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau lebih kontrol CIS Critical Security Controls IG1 v8. IG1 Kontrol CIS Critical Security Controls v8 dapat dikaitkan dengan beberapa AWS Config aturan. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.1	Membangun dan Memelihara Inventaris Aset Perusahaan Terperinci	terlampir eip	Aturan ini memastikan Elastic IPs dialokasikan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan. Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.
1.1	Membangun dan Memelihara Inventaris Aset Perusahaan Terperinci	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2)

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.
1.1	Membangun dan Memelihara Inventaris Aset Perusahaan Terperinci	vpc-network-acl-unused-periksa	Aturan ini memastikan bahwa daftar kontrol akses jaringan Amazon Virtual Private Cloud (VPC) sedang digunakan. Pemantauan untuk daftar kontrol akses jaringan yang tidak digunakan dapat membantu inventaris dan pengelolaan lingkungan Anda yang akurat.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.1	Membangun dan Memelihara Inventaris Aset Perusahaan Terperinci	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.1	Membangun dan Memelihara Inventaris Aset Perusahaan Terperinci	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.1	Membangun dan Memelihara Inventaris Aset Perusahaan Terperinci	ec2- -eni security-group-attached-to	Aturan ini memastikan grup keamanan dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) atau ke ENI. Aturan ini membantu memantau kelompok keamanan yang tidak digunakan dalam inventaris dan pengelolaan lingkungan Anda.
2.2	Pastikan Perangkat Lunak Resmi Saat Ini Didukung	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Pastikan Perangkat Lunak Resmi Saat Ini Didukung	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Pastikan Perangkat Lunak Resmi Saat Ini Didukung	ecs-fargate-latest-platform-versi	Pembaruan dan tambalan keamanan diterapkan secara otomatis untuk tugas Fargate AWS Anda. Jika ditemukan masalah keamanan yang memengaru hi versi platform AWS Fargate, AWS tambal versi platform. Untuk membantu pengelolaan tambalan tugas Amazon Elastic Container Service (ECS) yang menjalank an AWS Fargate, perbarui tugas mandiri layanan Anda untuk menggunakan versi platform terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.
3.3	Konfigurasikan Daftar Kontrol Akses Data	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.3	Konfigurasikan Daftar Kontrol Akses Data	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
3.3	Konfigurasikan Daftar Kontrol Akses Data	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.3	Konfigurasikan Daftar Kontrol Akses Data	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.3	Konfigurasikan Daftar Kontrol Akses Data	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	s3- account-level-publ ic-access -blok-per iodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
3.3	Konfigurasikan Daftar Kontrol Akses Data	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
3.3	Konfigurasikan Daftar Kontrol Akses Data	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
3.3	Konfigurasikan Daftar Kontrol Akses Data	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	ecs-task-definition-nonroot-pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan bahwa pengguna non-root ditunjuk untuk mengakses definisi tugas Amazon Elastic Container Service (Amazon ECS) Anda.
3.3	Konfigurasikan Daftar Kontrol Akses Data	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	efs-access-point-enforce-root-direktori	Menegakkan direktori root untuk jalur akses Amazon Elastic File System (Amazon EFS) membantu membatasi akses data dengan memastikan bahwa pengguna jalur akses hanya dapat menjangkau file dari subdirektori yang ditentukan.
3.4	Menegakkan Retensi Data	s3- version-lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihkan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4	Menegakkan Retensi Data	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.
4.1	Membangun dan Mempertahankan Proses Konfigurasi yang Aman	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Membangun dan Mempertahankan Proses Konfigurasi yang Aman	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.
4.1	Membangun dan Mempertahankan Proses Konfigurasi yang Aman	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Membangun dan Mempertahankan Proses Konfigurasi yang Aman	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Membangun dan Mempertahankan Proses Konfigurasi yang Aman	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Membangun dan Mempertahankan Proses Konfigurasi yang Aman	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Membangun dan Mempertahankan Proses Konfigurasi yang Aman	efs-access-point-enforce-root-direktori	Menegakkan direktori root untuk jalur akses Amazon Elastic File System (Amazon EFS) membantu membatasi akses data dengan memastikan bahwa pengguna jalur akses hanya dapat menjangkau file dari subdirektori yang ditentukan.
4.1	Membangun dan Mempertahankan Proses Konfigurasi yang Aman	secretsmanager-rotation-enabled-check	Aturan ini memastikan AWS rahasia Secrets Manager telah diaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Membangun dan Mempertahankan Proses Konfigurasi yang Aman	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.6	Mengelola Aset dan Perangkat Lunak Perusahaan dengan Aman	alb-http-to-https-pemeriksaan-pengalihan	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
4.6	Mengelola Aset dan Perangkat Lunak Perusahaan dengan Aman	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.6	Mengelola Aset dan Perangkat Lunak Perusahaan dengan Aman	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
4.6	Mengelola Aset dan Perangkat Lunak Perusahaan dengan Aman	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.6	Mengelola Aset dan Perangkat Lunak Perusahaan dengan Aman	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
4.6	Mengelola Aset dan Perangkat Lunak Perusahaan dengan Aman	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindung i data dalam perjalana n, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.7	Mengelola Akun Default pada Aset dan Perangkat Lunak Perusahaan	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.
5.1	Menetapkan dan Memelihara Inventari sasi Akun	account-part-of-or ganizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastika n bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.2	Gunakan Kata Sandi Unik	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.2	Gunakan Kata Sandi Unik	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.2	Gunakan Kata Sandi Unik	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.2	Gunakan Kata Sandi Unik	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.3	Nonaktifkan Akun Dormant	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.4	Batasi Hak Istimewa Administrator ke Akun Administrator Khusus	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.4	Batasi Hak Istimewa Administrator ke Akun Administrator Khusus	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.4	Memerlukan MFA untuk Akses Jaringan Jarak Jauh	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.4	Memerlukan MFA untuk Akses Jaringan Jarak Jauh	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.4	Memerlukan MFA untuk Akses Jaringan Jarak Jauh	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.5	Memerlukan MFA untuk Akses Administratif	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1	Membangun dan Mempertahankan Proses Manajemen Kerentanan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1	Membangun dan Mempertahankan Proses Manajemen Kerentanan	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1	Membangun dan Mempertahankan Proses Manajemen Kerentanan	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3	Lakukan Manajemen Patch Sistem Operasi Otomatis	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
7.3	Lakukan Manajemen Patch Sistem Operasi Otomatis	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3	Lakukan Manajemen Patch Sistem Operasi Otomatis	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.4	Lakukan Manajemen Patch Aplikasi Otomatis	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
7.4	Lakukan Manajemen Patch Aplikasi Otomatis	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.4	Lakukan Manajemen Patch Aplikasi Otomatis	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.1	Menetapkan dan Memelihara Proses Manajemen Log Audit	audit-log-policy-exists (Pemeriksaan proses)	Menetapkan dan memelihara kebijakan manajemen log audit yang menentukan persyaratan pencatatan organisasi Anda. Ini termasuk, namun tidak terbatas pada, peninjauan dan retensi log audit.
8.2	Kumpulkan Log Audit	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
8.2	Kumpulkan Log Audit	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
8.2	Kumpulkan Log Audit	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDbEncrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.
8.3	Pastikan Penyimpanan Log Audit yang Memadai	s3- version-lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihkan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.1	Menyebarkan dan Memelihara Perangkat Lunak Anti-Malware	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2	Konfigurasikan Pembaruan Tanda Tangan Anti-Malware Otomatis	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.
11.2	Lakukan Pencadangan Otomatis	s3- version-lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihkan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Lindungi Data Pemulihan	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
11.3	Lindungi Data Pemulihan	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
11.3	Lindungi Data Pemulihan	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Lindungi Data Pemulihan	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	s3- version-lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihk an objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Kontrol Keamanan Kritis CIS IG1 v8.

Praktik Terbaik Operasional untuk Kontrol Keamanan Kritis CIS v8 IG2

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini menyediakan contoh pemetaan antara Center for Internet Security (CIS) Critical Security Controls v8 dan aturan AWS Config IG2 terkelola. Masing-masing AWS Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau lebih kontrol CIS Critical Security Controls IG2 v8. IG2 Kontrol CIS Critical Security Controls v8 dapat dikaitkan dengan beberapa AWS Config aturan. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.1	Membangun dan Memelihara Inventaris Aset Perusahaan Terperinci	terlampir eip	Aturan ini memastikan Elastic IPs dialokasikan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan. Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.1	Membangun dan Memelihara Inventaris Aset Perusahaan Terperinci	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.
1.1	Membangun dan Memelihara Inventaris Aset Perusahaan Terperinci	vpc-network-acl-unused-periksa	Aturan ini memastikan bahwa daftar kontrol akses jaringan Amazon Virtual Private Cloud (VPC) sedang digunakan. Pemantauan untuk daftar kontrol akses jaringan yang tidak digunakan dapat membantu inventaris dan pengelolaan lingkungan Anda yang akurat.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.1	Membangun dan Memelihara Inventaris Aset Perusahaan Terperinci	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.1	Membangun dan Memelihara Inventaris Aset Perusahaan Terperinci	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.1	Membangun dan Memelihara Inventaris Aset Perusahaan Terperinci	ec2- -eni security-group-attached-to	Aturan ini memastikan grup keamanan dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) atau ke ENI. Aturan ini membantu memantau kelompok keamanan yang tidak digunakan dalam inventaris dan pengelolaan lingkungan Anda.
2.2	Pastikan Perangkat Lunak Resmi Saat Ini Didukung	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Pastikan Perangkat Lunak Resmi Saat Ini Didukung	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Pastikan Perangkat Lunak Resmi Saat Ini Didukung	ecs-fargate-latest-platform-versi	Pembaruan dan tambalan keamanan diterapkan secara otomatis untuk tugas Fargate AWS Anda. Jika ditemukan masalah keamanan yang memengaru hi versi platform AWS Fargate, AWS tambal versi platform. Untuk membantu pengelolaan tambalan tugas Amazon Elastic Container Service (ECS) yang menjalank an AWS Fargate, perbarui tugas mandiri layanan Anda untuk menggunakan versi platform terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.4	Memanfaatkan Alat Inventaris Perangkat Lunak Otomatis	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.4	Memanfaatkan Alat Inventaris Perangkat Lunak Otomatis	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.
3.3	Konfigurasikan Daftar Kontrol Akses Data	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.3	Konfigurasikan Daftar Kontrol Akses Data	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsageUsia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
3.3	Konfigurasikan Daftar Kontrol Akses Data	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.3	Konfigurasikan Daftar Kontrol Akses Data	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.3	Konfigurasikan Daftar Kontrol Akses Data	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	s3- account-level-publ ic-access -blok-per iodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
3.3	Konfigurasikan Daftar Kontrol Akses Data	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
3.3	Konfigurasikan Daftar Kontrol Akses Data	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
3.3	Konfigurasikan Daftar Kontrol Akses Data	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	ecs-task-definition-nonroot-pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan bahwa pengguna non-root ditunjuk untuk mengakses definisi tugas Amazon Elastic Container Service (Amazon ECS) Anda.
3.3	Konfigurasikan Daftar Kontrol Akses Data	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	efs-access-point-enforce-root-direktori	Menegakkan direktori root untuk jalur akses Amazon Elastic File System (Amazon EFS) membantu membatasi akses data dengan memastikan bahwa pengguna jalur akses hanya dapat menjangkau file dari subdirektori yang ditentukan.
3.4	Menegakkan Retensi Data	s3- version-lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihkan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4	Menegakkan Retensi Data	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.
3.10	Enkripsi Data Sensitif dalam Transit	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.10	Enkripsi Data Sensitif dalam Transit	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan Applicati on Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
3.10	Enkripsi Data Sensitif dalam Transit	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.10	Enkripsi Data Sensitif dalam Transit	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
3.10	Enkripsi Data Sensitif dalam Transit	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.10	Enkripsi Data Sensitif dalam Transit	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
3.10	Enkripsi Data Sensitif dalam Transit	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.10	Enkripsi Data Sensitif dalam Transit	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
3.10	Enkripsi Data Sensitif dalam Transit	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.10	Enkripsi Data Sensitif dalam Transit	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
3.11	Enkripsi Data Sensitif saat Istirahat	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.11	Enkripsi Data Sensitif saat Istirahat	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
3.11	Enkripsi Data Sensitif saat Istirahat	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
3.11	Enkripsi Data Sensitif saat Istirahat	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.11	Enkripsi Data Sensitif saat Istirahat	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
3.11	Enkripsi Data Sensitif saat Istirahat	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.11	Enkripsi Data Sensitif saat Istirahat	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
3.11	Enkripsi Data Sensitif saat Istirahat	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.11	Enkripsi Data Sensitif saat Istirahat	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
3.11	Enkripsi Data Sensitif saat Istirahat	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.11	Enkripsi Data Sensitif saat Istirahat	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.11	Enkripsi Data Sensitif saat Istirahat	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
3.11	Enkripsi Data Sensitif saat Istirahat	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.11	Enkripsi Data Sensitif saat Istirahat	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
3.11	Enkripsi Data Sensitif saat Istirahat	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.11	Enkripsi Data Sensitif saat Istirahat	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
3.11	Enkripsi Data Sensitif saat Istirahat	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.11	Enkripsi Data Sensitif saat Istirahat	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
4.1	Membangun dan Mempertahankan Proses Konfigurasi yang Aman	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Membangun dan Mempertahankan Proses Konfigurasi yang Aman	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.
4.1	Membangun dan Mempertahankan Proses Konfigurasi yang Aman	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Membangun dan Mempertahankan Proses Konfigurasi yang Aman	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Membangun dan Mempertahankan Proses Konfigurasi yang Aman	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Membangun dan Mempertahankan Proses Konfigurasi yang Aman	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Membangun dan Mempertahankan Proses Konfigurasi yang Aman	efs-access-point-enforce-root-direktori	Menegakkan direktori root untuk jalur akses Amazon Elastic File System (Amazon EFS) membantu membatasi akses data dengan memastikan bahwa pengguna jalur akses hanya dapat menjangkau file dari subdirektori yang ditentukan.
4.1	Membangun dan Mempertahankan Proses Konfigurasi yang Aman	secretsmanager-rotation-enabled-check	Aturan ini memastikan AWS rahasia Secrets Manager telah diaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Membangun dan Mempertahankan Proses Konfigurasi yang Aman	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.6	Mengelola Aset dan Perangkat Lunak Perusahaan dengan Aman	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan Applicati on Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
4.6	Mengelola Aset dan Perangkat Lunak Perusahaan dengan Aman	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.6	Mengelola Aset dan Perangkat Lunak Perusahaan dengan Aman	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
4.6	Mengelola Aset dan Perangkat Lunak Perusahaan dengan Aman	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.6	Mengelola Aset dan Perangkat Lunak Perusahaan dengan Aman	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
4.6	Mengelola Aset dan Perangkat Lunak Perusahaan dengan Aman	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindung i data dalam perjalana n, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.7	Kelola Akun Default pada Aset dan Perangkat Lunak Perusahaan	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.
5.1	Menetapkan dan Memelihara Inventari sasi Akun	account-part-of-or ganizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastika n bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.2	Gunakan Kata Sandi Unik	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.2	Gunakan Kata Sandi Unik	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.2	Gunakan Kata Sandi Unik	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.2	Gunakan Kata Sandi Unik	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.3	Nonaktifkan Akun Dormant	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsageUsia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.4	Batasi Hak Istimewa Administrator ke Akun Administrator Khusus	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.4	Batasi Hak Istimewa Administrator ke Akun Administrator Khusus	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.6	Memusatkan Manajemen Akun	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.
6.4	Memerlukan MFA untuk Akses Jaringan Jarak Jauh	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.4	Memerlukan MFA untuk Akses Jaringan Jarak Jauh	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.4	Memerlukan MFA untuk Akses Jaringan Jarak Jauh	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.5	Memerlukan MFA untuk Akses Administratif	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.7	Memusatkan Kontrol Akses	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.
7.1	Membangun dan Mempertahankan Proses Manajemen Kerentanan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1	Membangun dan Mempertahankan Proses Manajemen Kerentanan	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1	Membangun dan Mempertahankan Proses Manajemen Kerentanan	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3	Lakukan Manajemen Patch Sistem Operasi Otomatis	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
7.3	Lakukan Manajemen Patch Sistem Operasi Otomatis	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3	Lakukan Manajemen Patch Sistem Operasi Otomatis	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.4	Lakukan Manajemen Patch Aplikasi Otomatis	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
7.4	Lakukan Manajemen Patch Aplikasi Otomatis	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.4	Lakukan Manajemen Patch Aplikasi Otomatis	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7,5	Lakukan Pemindaian Kerentanan Otomatis Aset Perusahaan Internal	ecr-private-image-scanning-diaktifkan	Pemindaian gambar Amazon Elastic Container Repositor y (ECR) membantu mengidentifikasi kerentanan perangkat lunak dalam gambar kontainer Anda. Mengaktifkan pemindaian gambar pada repositori ECR menambahk an lapisan verifikasi untuk integritas dan keamanan gambar yang disimpan.
8.1	Menetapkan dan Memelihara Proses Manajemen Log Audit	audit-log-policy-exists (Pemeriksaan proses)	Menetapkan dan memelihara kebijakan manajemen log audit yang menentukan persyaratan pencatata n organisasi Anda. Ini termasuk, namun tidak terbatas pada, peninjauan dan retensi log audit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
8.2	Kumpulkan Log Audit	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
8.2	Kumpulkan Log Audit	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDbEncrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.
8.3	Pastikan Penyimpanan Log Audit yang Memadai	s3- version-lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihkan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.5	Kumpulkan Log Audit Terperinci	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.5	Kumpulkan Log Audit Terperinci	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.5	Kumpulkan Log Audit Terperinci	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
8.5	Kumpulkan Log Audit Terperinci	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.5	Kumpulkan Log Audit Terperinci	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
8.5	Kumpulkan Log Audit Terperinci	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.5	Kumpulkan Log Audit Terperinci	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.5	Kumpulkan Log Audit Terperinci	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.5	Kumpulkan Log Audit Terperinci	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.5	Kumpulkan Log Audit Terperinci	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.5	Kumpulkan Log Audit Terperinci	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDbEncrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.5	Kumpulkan Log Audit Terperinci	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.5	Kumpulkan Log Audit Terperinci	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
8.5	Kumpulkan Log Audit Terperinci	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.7	Kumpulkan Log Audit Permintaan URL	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.
8.9	Sentralisasi Log Audit	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.10	Mempertahankan Log Audit	s3- version-lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihkan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).
8.10	Mempertahankan Log Audit	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.1	Menyebarkan dan Memelihara Perangkat Lunak Anti-Malware	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2	Konfigurasikan Pembaruan Tanda Tangan Anti-Malware Otomatis	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4	Konfigurasikan Pemindaian Anti-Malware Otomatis dari Media yang Dapat Dilepas	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.6	Mengelola Perangkat Lunak Anti-Malware secara Terpusat	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.7	Gunakan Perangkat Lunak Anti-Malware Berbasis Perilaku	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan tambahan, kapasitas khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.
11.2	Lakukan Pencadangan Otomatis	s3- version-lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihkan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Lindungi Data Pemulihan	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
11.3	Lindungi Data Pemulihan	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
11.3	Lindungi Data Pemulihan	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Lindungi Data Pemulihan	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan tambahan, kapasitas khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	s3- version-lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihk an objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositor i data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	rds-cluster-multi-az-diaktifkan	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	elbv2-multiple-az	Elastic Load Balancing (ELB) secara otomatis mendistribusikan lalu lintas masuk Anda di beberapa target, seperti EC2 instance, kontainer, dan alamat IP, di zona ketersedi aan. Untuk memastika n ketersediaan tinggi, pastikan ELB Anda telah mendaftarkan instans dari beberapa Availability Zone.
12.3	Mengelola Infrastru ktur Jaringan dengan Aman	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.3	Mengelola Infrastru ktur Jaringan dengan Aman	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan Applicati on Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
12.3	Mengelola Infrastru ktur Jaringan dengan Aman	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.3	Mengelola Infrastru ktur Jaringan dengan Aman	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
12.3	Mengelola Infrastru ktur Jaringan dengan Aman	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.3	Mengelola Infrastru ktur Jaringan dengan Aman	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
12.3	Mengelola Infrastru ktur Jaringan dengan Aman	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.3	Mengelola Infrastruktur Jaringan dengan Aman	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
12.6	Penggunaan Manajemen Jaringan Aman dan Protokol Komunikasi	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.6	Penggunaan Manajemen Jaringan Aman dan Protokol Komunikasi	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan Applicati on Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
12.6	Penggunaan Manajemen Jaringan Aman dan Protokol Komunikasi	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.6	Penggunaan Manajemen Jaringan Aman dan Protokol Komunikasi	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
12.6	Penggunaan Manajemen Jaringan Aman dan Protokol Komunikasi	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.6	Penggunaan Manajemen Jaringan Aman dan Protokol Komunikasi	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
12.6	Penggunaan Manajemen Jaringan Aman dan Protokol Komunikasi	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.6	Penggunaan Manajemen Jaringan Aman dan Protokol Komunikasi	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
13.1	Memusatkan Peringatan Acara Keamanan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
13.1	Memusatkan Peringatan Acara Keamanan	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
13.3	Menerapkan Solusi Deteksi Intrusi Jaringan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
13.6	Kumpulkan Log Arus Lalu Lintas Jaringan	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
13.6	Kumpulkan Log Arus Lalu Lintas Jaringan	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16.1	Membangun dan Menjaga Proses Pengembangan Aplikasi yang Aman	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild . Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16.1	Membangun dan Menjaga Proses Pengembangan Aplikasi yang Aman	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredensyal masuk dalam lingkungan proyek Codebuild . AWS Gunakan OAuth alih-alih token akses pribadi atau kredensyal masuk untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.
16.1	Membangun dan Menjaga Proses Pengembangan Aplikasi yang Aman	codebuild-project-environment-privileged-periksa	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan lingkungan CodeBuild proyek Amazon Anda tidak mengaktifkan mode istimewa. Pengaturan ini harus dinonaktifkan untuk mencegah akses yang tidak diinginkan ke Docker APIs serta perangkat keras yang mendasarinya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16.1	Membangun dan Menjaga Proses Pengembangan Aplikasi yang Aman	codebuild-project-artifact-encryption	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk AWS CodeBuild artefak Anda.
16.1	Membangun dan Menjaga Proses Pengembangan Aplikasi yang Aman	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Kontrol Keamanan Kritis CIS IG2 v8.

Praktik Terbaik Operasional untuk Kontrol Keamanan Kritis CIS v8 IG3

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini menyediakan contoh pemetaan antara Center for Internet Security (CIS) Critical Security Controls v8 dan aturan AWS Config IG3 terkelola. Masing-masing AWS Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau lebih kontrol CIS Critical Security Controls IG3 v8. IG3 Kontrol CIS Critical Security Controls v8 dapat dikaitkan dengan beberapa AWS Config aturan. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.1	Membangun dan Memelihara Inventaris Aset Perusahaan Terperinci	terlampir eip	Aturan ini memastikan Elastic IPs dialokasikan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan. Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.
1.1	Membangun dan Memelihara Inventaris Aset Perusahaan Terperinci	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			dengan standar organisasi Anda.
1.1	Membangun dan Memelihara Inventaris Aset Perusahaan Terperinci	vpc-network-acl-unused-periksa	Aturan ini memastikan bahwa daftar kontrol akses jaringan Amazon Virtual Private Cloud (VPC) sedang digunakan. Pemantauan untuk daftar kontrol akses jaringan yang tidak digunakan dapat membantu inventaris dan pengelolaan lingkungan Anda yang akurat.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.1	Membangun dan Memelihara Inventaris Aset Perusahaan Terperinci	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.1	Membangun dan Memelihara Inventaris Aset Perusahaan Terperinci	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.1	Membangun dan Memelihara Inventaris Aset Perusahaan Terperinci	ec2- -eni security-group-attached-to	Aturan ini memastikan grup keamanan dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) atau ke ENI. Aturan ini membantu memantau kelompok keamanan yang tidak digunakan dalam inventaris dan pengelolaan lingkungan Anda.
2.2	Pastikan Perangkat Lunak Resmi Saat Ini Didukung	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Pastikan Perangkat Lunak Resmi Saat Ini Didukung	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Pastikan Perangkat Lunak Resmi Saat Ini Didukung	ecs-fargate-latest-platform-versi	Pembaruan dan tambalan keamanan diterapkan secara otomatis untuk tugas Fargate AWS Anda. Jika ditemukan masalah keamanan yang memengaru hi versi platform AWS Fargate, AWS tambal versi platform. Untuk membantu pengelolaan tambalan tugas Amazon Elastic Container Service (ECS) yang menjalank an AWS Fargate, perbarui tugas mandiri layanan Anda untuk menggunakan versi platform terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.4	Memanfaatkan Alat Inventaris Perangkat Lunak Otomatis	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.4	Memanfaatkan Alat Inventaris Perangkat Lunak Otomatis	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.
3.3	Konfigurasikan Daftar Kontrol Akses Data	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.3	Konfigurasikan Daftar Kontrol Akses Data	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
3.3	Konfigurasikan Daftar Kontrol Akses Data	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.3	Konfigurasikan Daftar Kontrol Akses Data	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
3.3	Konfigurasikan Daftar Kontrol Akses Data	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
3.3	Konfigurasikan Daftar Kontrol Akses Data	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
3.3	Konfigurasikan Daftar Kontrol Akses Data	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	ecs-task-definition-nonroot-pengguna	Untuk membantu menerapkan prinsip hak istimewa terkecil, pastikan bahwa pengguna non-root ditunjuk untuk mengakses definisi tugas Amazon Elastic Container Service (Amazon ECS).
3.3	Konfigurasikan Daftar Kontrol Akses Data	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Konfigurasikan Daftar Kontrol Akses Data	efs-access-point-enforce-root-direktori	Menegakkan direktori root untuk jalur akses Amazon Elastic File System (Amazon EFS) membantu membatasi akses data dengan memastikan bahwa pengguna jalur akses hanya dapat menjangkau file dari subdirektori yang ditentukan.
3.4	Menegakkan Retensi Data	s3- version-lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihkan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4	Menegakkan Retensi Data	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.
3.10	Enkripsi Data Sensitif dalam Transit	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.10	Enkripsi Data Sensitif dalam Transit	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
3.10	Enkripsi Data Sensitif dalam Transit	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.10	Enkripsi Data Sensitif dalam Transit	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
3.10	Enkripsi Data Sensitif dalam Transit	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.10	Enkripsi Data Sensitif dalam Transit	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
3.10	Enkripsi Data Sensitif dalam Transit	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.10	Enkripsi Data Sensitif dalam Transit	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
3.10	Enkripsi Data Sensitif dalam Transit	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.10	Enkripsi Data Sensitif dalam Transit	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
3.11	Enkripsi Data Sensitif saat Istirahat	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.11	Enkripsi Data Sensitif saat Istirahat	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
3.11	Enkripsi Data Sensitif saat Istirahat	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
3.11	Enkripsi Data Sensitif saat Istirahat	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.11	Enkripsi Data Sensitif saat Istirahat	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
3.11	Enkripsi Data Sensitif saat Istirahat	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.11	Enkripsi Data Sensitif saat Istirahat	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
3.11	Enkripsi Data Sensitif saat Istirahat	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.11	Enkripsi Data Sensitif saat Istirahat	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
3.11	Enkripsi Data Sensitif saat Istirahat	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.11	Enkripsi Data Sensitif saat Istirahat	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.11	Enkripsi Data Sensitif saat Istirahat	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
3.11	Enkripsi Data Sensitif saat Istirahat	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.11	Enkripsi Data Sensitif saat Istirahat	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
3.11	Enkripsi Data Sensitif saat Istirahat	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.11	Enkripsi Data Sensitif saat Istirahat	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
3.11	Enkripsi Data Sensitif saat Istirahat	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.11	Enkripsi Data Sensitif saat Istirahat	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
3.14	Akses Data Sensitif Log	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14	Akses Data Sensitif Log	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14	Akses Data Sensitif Log	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
3.14	Akses Data Sensitif Log	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14	Akses Data Sensitif Log	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
3.14	Akses Data Sensitif Log	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14	Akses Data Sensitif Log	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14	Akses Data Sensitif Log	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14	Akses Data Sensitif Log	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14	Akses Data Sensitif Log	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14	Akses Data Sensitif Log	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDbEncrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14	Akses Data Sensitif Log	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14	Akses Data Sensitif Log	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
3.14	Akses Data Sensitif Log	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Membangun dan Mempertahankan Proses Konfigurasi yang Aman	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.
4.1	Membangun dan Mempertahankan Proses Konfigurasi yang Aman	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Membangun dan Mempertahankan Proses Konfigurasi yang Aman	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Membangun dan Mempertahankan Proses Konfigurasi yang Aman	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Membangun dan Mempertahankan Proses Konfigurasi yang Aman	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Membangun dan Mempertahankan Proses Konfigurasi yang Aman	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Membangun dan Mempertahankan Proses Konfigurasi yang Aman	efs-access-point-enforce-root-direktori	Menegakkan direktori root untuk jalur akses Amazon Elastic File System (Amazon EFS) membantu membatasi akses data dengan memastikan bahwa pengguna jalur akses hanya dapat menjangkau file dari subdirektori yang ditentukan.
4.1	Membangun dan Mempertahankan Proses Konfigurasi yang Aman	secretsmanager-rotation-enabled-check	Aturan ini memastikan AWS rahasia Secrets Manager telah diaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Membangun dan Mempertahankan Proses Konfigurasi yang Aman	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.6	Mengelola Aset dan Perangkat Lunak Perusahaan dengan Aman	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
4.6	Mengelola Aset dan Perangkat Lunak Perusahaan dengan Aman	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.6	Mengelola Aset dan Perangkat Lunak Perusahaan dengan Aman	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
4.6	Mengelola Aset dan Perangkat Lunak Perusahaan dengan Aman	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.6	Mengelola Aset dan Perangkat Lunak Perusahaan dengan Aman	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
4.6	Mengelola Aset dan Perangkat Lunak Perusahaan dengan Aman	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindung i data dalam perjalana n, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.7	Kelola Akun Default pada Aset dan Perangkat Lunak Perusahaan	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.
5.1	Menetapkan dan Memelihara Inventari sasi Akun	account-part-of-or ganizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastika n bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.2	Gunakan Kata Sandi Unik	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.2	Gunakan Kata Sandi Unik	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.2	Gunakan Kata Sandi Unik	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredensi masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.2	Gunakan Kata Sandi Unik	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.3	Nonaktifkan Akun Dormant	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.4	Batasi Hak Istimewa Administrator ke Akun Administrator Khusus	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.4	Batasi Hak Istimewa Administrator ke Akun Administrator Khusus	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.6	Memusatkan Manajemen Akun	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.
6.4	Memerlukan MFA untuk Akses Jaringan Jarak Jauh	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.4	Memerlukan MFA untuk Akses Jaringan Jarak Jauh	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredensi masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.4	Memerlukan MFA untuk Akses Jaringan Jarak Jauh	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.5	Memerlukan MFA untuk Akses Administratif	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.7	Memusatkan Kontrol Akses	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.
7.1	Membangun dan Mempertahankan Proses Manajemen Kerentanan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1	Membangun dan Mempertahankan Proses Manajemen Kerentanan	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1	Membangun dan Mempertahankan Proses Manajemen Kerentanan	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3	Lakukan Manajemen Patch Sistem Operasi Otomatis	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
7.3	Lakukan Manajemen Patch Sistem Operasi Otomatis	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3	Lakukan Manajemen Patch Sistem Operasi Otomatis	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.4	Lakukan Manajemen Patch Aplikasi Otomatis	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
7.4	Lakukan Manajemen Patch Aplikasi Otomatis	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.4	Lakukan Manajemen Patch Aplikasi Otomatis	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.5	Lakukan Pemindaian Kerentanan Otomatis Aset Perusahaan Internal	ecr-private-image-scanning-diaktifkan	Pemindaian gambar Amazon Elastic Container Repositor y (ECR) membantu mengidentifikasi kerentanan perangkat lunak dalam gambar kontainer Anda. Mengaktifkan pemindaian gambar pada repositori ECR menambahk an lapisan verifikasi untuk integritas dan keamanan gambar yang disimpan.
8.1	Menetapkan dan Memelihara Proses Manajemen Log Audit	audit-log-policy-exists (Pemeriksaan proses)	Menetapkan dan memelihara kebijakan manajemen log audit yang menentukan persyaratan pencatata n organisasi Anda. Ini termasuk, namun tidak terbatas pada, peninjauan dan retensi log audit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
8.2	Kumpulkan Log Audit	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
8.2	Kumpulkan Log Audit	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2	Kumpulkan Log Audit	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.
8.3	Pastikan Penyimpanan Log Audit yang Memadai	s3- version-lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihkan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.5	Kumpulkan Log Audit Terperinci	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.5	Kumpulkan Log Audit Terperinci	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.5	Kumpulkan Log Audit Terperinci	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
8.5	Kumpulkan Log Audit Terperinci	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.5	Kumpulkan Log Audit Terperinci	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
8.5	Kumpulkan Log Audit Terperinci	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.5	Kumpulkan Log Audit Terperinci	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.5	Kumpulkan Log Audit Terperinci	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.5	Kumpulkan Log Audit Terperinci	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.5	Kumpulkan Log Audit Terperinci	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.5	Kumpulkan Log Audit Terperinci	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.5	Kumpulkan Log Audit Terperinci	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.5	Kumpulkan Log Audit Terperinci	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
8.5	Kumpulkan Log Audit Terperinci	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.7	Kumpulkan Log Audit Permintaan URL	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.
8.9	Sentralisasi Log Audit	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.10	Mempertahankan Log Audit	s3- version-lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihkan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).
8.10	Mempertahankan Log Audit	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.1	Menyebarkan dan Memelihara Perangkat Lunak Anti-Malware	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2	Konfigurasikan Pembaruan Tanda Tangan Anti-Malware Otomatis	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4	Konfigurasikan Pemindaian Anti-Malware Otomatis dari Media yang Dapat Dilepas	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.6	Mengelola Perangkat Lunak Anti-Malware secara Terpusat	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.7	Gunakan Perangkat Lunak Anti-Malware Berbasis Perilaku	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	Lakukan Pencadangan Otomatis	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.
11.2	Lakukan Pencadangan Otomatis	s3- version-lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihkan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Lindungi Data Pemulihan	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
11.3	Lindungi Data Pemulihan	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
11.3	Lindungi Data Pemulihan	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Lindungi Data Pemulihan	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.
11.4	Membangun dan Mempertahankan Instance Data Pemulihan yang Terisolasi	s3- version-lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihk an objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	dibatasi ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	s3- account-level-publ ic-access -blok-per iodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositor i data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	rds-cluster-multi-az-diaktifkan	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.2	Membangun dan Memelihara Arsitektur Jaringan yang Aman	elbv2-multiple-az	Elastic Load Balancing (ELB) secara otomatis mendistribusikan lalu lintas masuk Anda di beberapa target, seperti EC2 instance, kontainer, dan alamat IP, di zona ketersedi aan. Untuk memastika n ketersediaan tinggi, pastikan ELB Anda telah mendaftarkan instans dari beberapa Availability Zone.
12.3	Mengelola Infrastru ktur Jaringan dengan Aman	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.3	Mengelola Infrastru ktur Jaringan dengan Aman	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
12.3	Mengelola Infrastru ktur Jaringan dengan Aman	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.3	Mengelola Infrastru ktur Jaringan dengan Aman	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
12.3	Mengelola Infrastru ktur Jaringan dengan Aman	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.3	Mengelola Infrastru ktur Jaringan dengan Aman	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
12.3	Mengelola Infrastru ktur Jaringan dengan Aman	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.3	Mengelola Infrastruktur Jaringan dengan Aman	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
12.6	Penggunaan Manajemen Jaringan Aman dan Protokol Komunikasi	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.6	Penggunaan Manajemen Jaringan Aman dan Protokol Komunikasi	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
12.6	Penggunaan Manajemen Jaringan Aman dan Protokol Komunikasi	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.6	Penggunaan Manajemen Jaringan Aman dan Protokol Komunikasi	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
12.6	Penggunaan Manajemen Jaringan Aman dan Protokol Komunikasi	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.6	Penggunaan Manajemen Jaringan Aman dan Protokol Komunikasi	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
12.6	Penggunaan Manajemen Jaringan Aman dan Protokol Komunikasi	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.6	Penggunaan Manajemen Jaringan Aman dan Protokol Komunikasi	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
13.1	Memusatkan Peringatan Acara Keamanan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
13.1	Memusatkan Peringatan Acara Keamanan	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
13.3	Menerapkan Solusi Deteksi Intrusi Jaringan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
13.6	Kumpulkan Log Arus Lalu Lintas Jaringan	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
13.6	Kumpulkan Log Arus Lalu Lintas Jaringan	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
13.10	Lakukan Penyaringan Lapisan Aplikasi	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindungi nya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16.1	Membangun dan Menjaga Proses Pengembangan Aplikasi yang Aman	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild . Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16.1	Membangun dan Menjaga Proses Pengembangan Aplikasi yang Aman	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredensyal masuk dalam lingkungan proyek Codebuild . AWS Gunakan OAuth alih-alih token akses pribadi atau kredensyal masuk untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.
16.1	Membangun dan Menjaga Proses Pengembangan Aplikasi yang Aman	codebuild-project-environment-privileged-periksa	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan lingkungan CodeBuild proyek Amazon Anda tidak mengaktifkan mode istimewa. Pengaturan ini harus dinonaktifkan untuk mencegah akses yang tidak diinginkan ke Docker APIs serta perangkat keras yang mendasarinya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16.1	Membangun dan Menjaga Proses Pengembangan Aplikasi yang Aman	codebuild-project-artifact-encryption	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk AWS CodeBuild artefak Anda.
16.1	Membangun dan Menjaga Proses Pengembangan Aplikasi yang Aman	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16.12	Menerapkan Pemeriksaan Keamanan Tingkat Kode	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild . Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16.12	Menerapkan Pemeriksaan Keamanan Tingkat Kode	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredensyal masuk dalam lingkungan proyek Codebuild . AWS Gunakan OAuth alih-alih token akses pribadi atau kredensyal masuk untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.
16.12	Menerapkan Pemeriksaan Keamanan Tingkat Kode	codebuild-project-environment-privileged-periksa	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan lingkungan CodeBuild proyek Amazon Anda tidak mengaktifkan mode istimewa. Pengaturan ini harus dinonaktifkan untuk mencegah akses yang tidak diinginkan ke Docker APIs serta perangkat keras yang mendasarinya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16.12	Menerapkan Pemeriksaan Keamanan Tingkat Kode	codebuild-project-artifact-encryption	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk AWS CodeBuild artefak Anda.
16.12	Menerapkan Pemeriksaan Keamanan Tingkat Kode	codebuild-project-logging-enabled	Pastikan pencatata n AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatc h atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Kontrol Keamanan Kritis CIS IG3 v8.

Praktik Terbaik Operasional untuk CIS Top 20

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini menyediakan contoh pemetaan antara 20 Kontrol Keamanan Kritis Teratas Center for Internet Security (CIS) dan aturan AWS Config terkelola. Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan berhubungan dengan satu atau beberapa kontrol CIS Top 20. Kontrol CIS Top 20 dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

Paket Kesesuaian ini divalidasi oleh AWS Security Assurance Services LLC (AWS SAS), yang merupakan tim dari Payment Card Industry Qualified Security Assesors (QSAs), HITRUST Certified Common Security Framework Practitioners (CCSFPs), dan profesional kepatuhan yang disertifikasi untuk memberikan panduan dan penilaian untuk berbagai kerangka kerja industri. AWS Profesional SAS merancang Paket Kesesuaian ini untuk memungkinkan pelanggan menyelaraskan dengan subset dari CIS Top 20.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.2	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.
CIS.2	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal

ID Kontrol	AWS Config Aturan	Bimbingan
		kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
CIS.2	ec2- -eni security-group-attached-to	Aturan ini memastikan grup keamanan dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) atau ke ENI. Aturan ini membantu memantau kelompok keamanan yang tidak digunakan dalam inventaris dan pengelolaan lingkungan Anda.
CIS.2	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan , sesuai dengan standar organisasi Anda.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.2	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirk an ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.
CIS.2	terlampir eip	Aturan ini memastikan Elastic IPs dialokasikan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan . Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.3	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
CIS.3	guardduty-non-archived-find ings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan: rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighS ev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.3	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
CIS.4	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
CIS.4	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.4	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensyal masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
CIS.4	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.4	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
CIS.5	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.5	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapka n status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigura si aplikasi, dan detail lainnya tentang lingkungan Anda.
CIS.5	ec2- -periksa managedin stance-patch-compliance-sta tus	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.5	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.5	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00 -sat: 16:30), dan automated SnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
CIS.6	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.6	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
CIS.6	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.6	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.
CIS.6	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.6	cloudwatch-alarm-action-check	Amazon CloudWatch memperingatkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.
CIS.6	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.6	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
CIS.6	guardduty-non-archived-find ings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan: rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighS ev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.6	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua Wilayah AWS ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.6	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.6	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.6	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
CIS.6	vpc-flow-logs-enabled	Log aliran VPC menyediak an catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.8	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
CIS.9	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CIS.9	ebs-snapshot-public-restora ble-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihka n secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.9	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CIS.9	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
CIS.9	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.9	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.9	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.9	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkin kan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabk an akses tidak sah ke sumber daya VPC Amazon.
CIS.9	lambda-function-public-acce ss-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.9	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyarat an untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.
CIS.9	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.9	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
CIS.9	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.9	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,338 9,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.9	s3- -blok account-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
CIS.9	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.9	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
CIS.9	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.9	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .
CIS.9	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.10	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.
CIS.10	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadang an berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.10	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.
CIS.10	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.10	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihka n setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.
CIS.11	ec2- -eni security-group-att ached-to	Aturan ini memastikan grup keamanan dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) atau ke ENI. Aturan ini membantu memantau kelompok keamanan yang tidak digunakan dalam inventaris dan pengelolaan lingkungan Anda.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.11	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.
CIS.11	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.11	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .
CIS.11	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.12	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CIS.12	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CIS.12	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.12	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearc h Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
CIS.12	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.12	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
CIS.12	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.12	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.12	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkin kan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabk an akses tidak sah ke sumber daya VPC Amazon.
CIS.12	lambda-function-public-acce ss-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.12	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyarat an untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.
CIS.12	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.12	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
CIS.12	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.12	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,338 9,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.12	s3- -blok account-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
CIS.12	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.12	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
CIS.12	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.12	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
CIS.12	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.12	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.
CIS.13	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.13	alb-http-to-https-pengalihan-periksa	Untuk membantu melindung i data dalam perjalanan, pastikan Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
CIS.13	api-gw-cache-enabled-dan-di enkripsi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CIS.13	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
CIS.13	cloudwatch-log-group-encryp ted	Untuk membantu melindung i data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.13	ec2- ebs-encryption-by-default	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CIS.13	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
CIS.13	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.13	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindung i data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
CIS.13	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
CIS.13	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.13	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.
CIS.13	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CIS.13	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.13	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
CIS.13	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.13	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.
CIS.13	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
CIS.13	s3- bucket-ssl-requests-only	Untuk membantu melindung i data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerluka n permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.13	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CIS.13	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.13	sns-encrypted-kms	Untuk membantu melindung i data saat istirahat, pastikan topik Amazon Simple Notificat ion Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CIS.14	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastika n sertifikat X509 dikeluark an oleh AWS ACM. Sertifika t ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.14	alb-http-to-https-pengalihan-periksa	Untuk membantu melindung i data dalam perjalanan, pastikan Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
CIS.14	api-gw-cache-enabled-dan-di enkripsi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CIS.14	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
CIS.14	cloudwatch-log-group-encryp ted	Untuk membantu melindung i data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.14	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CIS.14	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CIS.14	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.14	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastika n instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CIS.14	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
CIS.14	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.14	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindung i data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.14	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribus i kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertah ankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.
CIS.14	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.14	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.
CIS.14	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
CIS.14	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.14	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
CIS.14	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CIS.14	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.14	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
CIS.14	s3- -blok account-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.14	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.
CIS.14	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_ bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs
CIS.14	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.14	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
CIS.14	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
CIS.14	s3- bucket-ssl-requests-only	Untuk membantu melindung i data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerluka n permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.14	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CIS.14	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.14	sns-encrypted-kms	Untuk membantu melindung i data saat istirahat, pastikan topik Amazon Simple Notificat ion Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CIS.16	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaima na ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.16	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penol akan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilka n, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.16	cloudwatch-alarm-action-check	Amazon CloudWatch memperingatkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.16	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribus i kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertah ankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.16	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
CIS.16	guardduty-non-archived-find ings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan: rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighS ev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.16	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan Centers for Internet Security (CIS) AWS Foundations Benchmark untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Config Aturan	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
CIS.16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.16	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.
CIS.16	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.16	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
CIS.16	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurang i peluang bagi identitas untuk menerima atau mempertah ankan hak istimewa yang berlebihan.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.16	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentif ikasi, Anda harus menonakti fkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.16	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensyal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
CIS.16	root-account-hardware-mfa-d iaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan ekstra untuk kredensyal masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.16	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifka n untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
CIS.16	secretsmanager-rotation-ena bled-check	Aturan ini memastikan AWS rahasia Secrets Manager telah diaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotens i mengurangi dampak bisnis jika rahasia itu dikomprom ikan.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.16	secretsmanager-scheduled-rotation-success-periksa	Aturan ini memastikan bahwa AWS rahasia Secrets Manager telah berhasil diputar sesuai dengan jadwal rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode di mana rahasia aktif, dan berpotensi mengurangi dampak bisnis jika dikomprom ikan.
CIS.16	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.18	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild. Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.
CIS.18	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredensyal masuk dalam lingkungan proyek Codebuild. AWS Gunakan OAuth alih-alih token akses pribadi atau kredensyal masuk untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.19	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
CIS.19	guardduty-non-archived-find ings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan: rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighS ev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	AWS Config Aturan	Bimbingan
CIS.19	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
CIS.2	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk CIS Top 20.

Praktik Terbaik Operasional untuk CISA Cyber Essentials

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara Cybersecurity & Infrastructure Security Agency (CISA) Cyber Essentials (CE) dan aturan Config terkelola. AWS Setiap AWS Config aturan berlaku untuk AWS sumber daya tertentu, dan berhubungan dengan satu atau lebih kontrol CISA CE. Kontrol CISA CE dapat dikaitkan dengan beberapa AWS Config aturan. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Staf Anda-1	Kembangkan budaya kesadaran untuk mendorong karyawan membuat pilihan yang baik secara online.	security-awareness-program-exists(Pemeriksaan Proses)	Membangun dan memelihara program kesadaran keamanan untuk organisasi Anda. Program kesadaran keamanan mendidik karyawan tentang cara melindungi organisasi mereka dari berbagai pelanggaran atau insiden keamanan.
Staf Anda-2	Pelajari tentang risiko seperti phishing dan	security-awareness-program-exists(Pemeriksaan Proses)	Membangun dan memelihara program kesadaran keamanan

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	kompromi email bisnis.xxxxx.		untuk organisasi Anda. Program kesadaran keamanan mendidik karyawan tentang cara melindungi organisasi mereka dari berbagai pelanggaran atau insiden keamanan.
Staf Anda-3	Pertahankan kesadaran akan peristiwa terkini yang terkait dengan keamanan siber, menggunakan peristiwa yang dipelajari dan dilaporkan untuk tetap waspada terhadap lingkungan ancaman saat ini dan gesit terhadap tren keamanan siber.	security-awareness-program-exists(Pemeriksaan Proses)	Membangun dan memelihara program kesadaran keamanan untuk organisasi Anda. Program kesadaran keamanan mendidik karyawan tentang cara melindungi organisasi mereka dari berbagai pelanggaran atau insiden keamanan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Staf Anda-4	Manfaatkan pelatihan keamanan siber dasar untuk meningkatkan paparan konsep, terminologi, dan aktivitas keamanan siber yang terkait dengan penerapan praktik terbaik keamanan siber.	security-awareness-program-exists(Pemeriksaan Proses)	Membangun dan memelihara program kesadaran keamanan untuk organisasi Anda. Program kesadaran keamanan mendidik karyawan tentang cara melindungi organisasi mereka dari berbagai pelanggaran atau insiden keamanan.
Staf Anda-5	Mengidentifikasi sumber daya pelatihan yang tersedia melalui asosiasi profesional, lembaga akademik, sektor swasta dan sumber-sumber pemerintah.	security-awareness-program-exists(Pemeriksaan Proses)	Membangun dan memelihara program kesadaran keamanan untuk organisasi Anda. Program kesadaran keamanan mendidik karyawan tentang cara melindungi organisasi mereka dari berbagai pelanggaran atau insiden keamanan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-1	Pelajari apa yang ada di jaringan Anda. Pertahankan inventaris aset perangkat keras dan perangkat lunak untuk mengetahui apa yang sedang dimainkan dan berisiko dari serangan.	terlampir eip	Aturan ini memastikan Elastic IPs dialokasikan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan. Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.
Sistem Anda-1	Pelajari apa yang ada di jaringan Anda. Pertahankan inventaris aset perangkat keras dan perangkat lunak untuk mengetahui apa yang sedang dimainkan dan berisiko dari serangan.	vpc-network-acl-unused-periksa	Aturan ini memastikan bahwa daftar kontrol akses jaringan Amazon Virtual Private Cloud (VPC) sedang digunakan. Pemantauan untuk daftar kontrol akses jaringan yang tidak digunakan dapat membantu inventaris dan pengelolaan lingkungan Anda yang akurat.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-1	Pelajari apa yang ada di jaringan Anda. Pertahankan inventaris aset perangkat keras dan perangkat lunak untuk mengetahui apa yang sedang dimainkan dan berisiko dari serangan.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-1	Pelajari apa yang ada di jaringan Anda. Pertahankan inventaris aset perangkat keras dan perangkat lunak untuk mengetahui apa yang sedang dimainkan dan berisiko dari serangan.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-1	Pelajari apa yang ada di jaringan Anda. Pertahankan inventaris aset perangkat keras dan perangkat lunak untuk mengetahui apa yang sedang dimainkan dan berisiko dari serangan.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
Sistem Anda-1	Pelajari apa yang ada di jaringan Anda. Pertahankan inventaris aset perangkat keras dan perangkat lunak untuk mengetahui apa yang sedang dimainkan dan berisiko dari serangan.	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-1	Pelajari apa yang ada di jaringan Anda. Pertahankan inventaris aset perangkat keras dan perangkat lunak untuk mengetahui apa yang sedang dimainkan dan berisiko dari serangan.	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-2	Manfaatkan pembaruan otomatis untuk semua sistem operasi dan perangkat lunak pihak ketiga.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
Sistem Anda-2	Manfaatkan pembaruan otomatis untuk semua sistem operasi dan perangkat lunak pihak ketiga.	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-2	Manfaatkan pembaruan otomatis untuk semua sistem operasi dan perangkat lunak pihak ketiga.	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-2	Manfaatkan pembaruan otomatis untuk semua sistem operasi dan perangkat lunak pihak ketiga.	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relational Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindungi nya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	codebuild-project-envvar-awscred-periksa	Pastikan kredensial otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild. Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredenal masuk dalam lingkungan proyek Codebuild . AWS Gunakan OAuth alih-alih token akses pribadi atau kredensyal masuk untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	opensearch-data-node-fault-toleransi	Amazon OpenSearch Service (OpenSearch Service) memerlukan setidaknya tiga node data untuk ketersediaan tinggi dan toleransi kesalahan. Menyebarkan domain OpenSearch Layanan dengan setidaknya tiga node data memastikan operasi klaster jika node gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi, pengembalian, dan pendelegasian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigura si keamanan untuk semua aset perangkat keras dan perangkat lunak.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigura si keamanan untuk semua aset perangkat keras dan perangkat lunak.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relational Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	rds-cluster-multi-az-diaktifkan	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigura si keamanan untuk semua aset perangkat keras dan perangkat lunak.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	secretsmanager-rotation-enabled-check	Aturan ini memastikan AWS rahasia Secrets Manager telah diaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan.
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	secretsmanager-secret-periodic-rotation	Aturan ini memastikan AWS rahasia Secrets Manager mengaktifkan rotasi periodik. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan. Nilai defaultnya adalah 90 hari.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	secretsmanager-secret-unused	Jika kredensil yang tidak digunakan ada di AWS Secrets Manager, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini memungkinkan Anda untuk menetapkan nilai ke unusedFor Days (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	dynamodb-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-3	Menerapkan konfigurasi keamanan untuk semua aset perangkat keras dan perangkat lunak.	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Sistem Anda-4	Hapus perangkat keras dan perangkat lunak yang tidak didukung atau tidak sah dari sistem.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lingkungan Anda-1	Pelajari siapa yang ada di jaringan Anda. Menjaga inventaris koneksi jaringan (pengguna, vendor, mitra bisnis, dll.).	terlampir eip	Aturan ini memastikan Elastic IPs dialokasikan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan. Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.
Lingkungan Anda-1	Pelajari siapa yang ada di jaringan Anda. Menjaga inventaris koneksi jaringan (pengguna, vendor, mitra bisnis, dll.).	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lingkungan Anda-1	Pelajari siapa yang ada di jaringan Anda. Menjaga inventaris koneksi jaringan (pengguna, vendor, mitra bisnis, dll.).	vpc-network-acl-unused-periksa	Aturan ini memastikan bahwa daftar kontrol akses jaringan Amazon Virtual Private Cloud (VPC) sedang digunakan. Pemantauan untuk daftar kontrol akses jaringan yang tidak digunakan dapat membantu inventaris dan pengelolaan lingkungan Anda yang akurat.
Lingkungan Anda-2	Manfaatkan otentikasi multi-faktor untuk semua pengguna, dimulai dengan pengguna akses istimewa, administratif, dan jarak jauh.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lingkungan Anda-2	Manfaatkan otentikasi multi-faktor untuk semua pengguna, dimulai dengan pengguna akses istimewa, administratif, dan jarak jauh.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lingkungan Anda-2	Manfaatkan otentikasi multi-faktor untuk semua pengguna, dimulai dengan pengguna akses istimewa, administratif, dan jarak jauh.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lingkungan Anda-2	Manfaatkan otentikasi multi-faktor untuk semua pengguna, dimulai dengan pengguna akses istimewa, administratif, dan jarak jauh.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lingkungan Anda-3	Berikan akses dan izin admin berdasarkan hak istimewa need-to-know dan paling sedikit.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lingkungan Anda-3	Berikan akses dan izin admin berdasarkan hak istimewa need-to-know dan paling sedikit.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lingkungan Anda-3	Berikan akses dan izin admin berdasarkan hak istimewa need-to-know dan paling sedikit.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
Lingkungan Anda-3	Berikan akses dan izin admin berdasarkan hak istimewa need-to-know dan paling sedikit.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lingkungan Anda-3	Berikan akses dan izin admin berdasarkan hak istimewa need-to-know dan paling sedikit.	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lingkungan Anda-3	Berikan akses dan izin admin berdasarkan hak istimewa need-to-know dan paling sedikit.	secretsmanager-secret-unused	Jika kredensil yang tidak digunakan ada di AWS Secrets Manager, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini memungkinkan Anda untuk menetapkan nilai ke unusedFor Days (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lingkungan Anda-3	Berikan akses dan izin admin berdasarkan hak istimewa need-to-know dan paling sedikit.	opensearch-access-control-enabled	Pastikan kontrol akses berbutir halus diaktifkan di domain Layanan Amazon OpenSearch Anda. Kontrol akses berbutir halus menyediakan mekanisme otorisasi yang disempurnakan untuk mencapai akses yang paling tidak memiliki hak istimewa ke domain Layanan Amazon. OpenSearch Ini memungkinkan kontrol akses berbasis peran ke domain, serta indeks, dokumen, dan keamanan tingkat lapangan, dukungan untuk dasbor OpenSearch Layanan multi-tenancy, dan otentikasi dasar HTTP untuk Layanan dan Kibana. OpenSearch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Lingkungan Anda-4	Manfaatkan kata sandi unik untuk semua pengguna.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-1 Anda	Pelajari bagaimana data Anda dilindungi.	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.
Data-1 Anda	Pelajari bagaimana data Anda dilindungi.	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-1 Anda	Pelajari bagaimana data Anda dilindungi.	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
Data-1 Anda	Pelajari bagaimana data Anda dilindungi.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-1 Anda	Pelajari bagaimana data Anda dilindungi.	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Data-1 Anda	Pelajari bagaimana data Anda dilindungi.	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-1 Anda	Pelajari bagaimana data Anda dilindungi.	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
Data-1 Anda	Pelajari bagaimana data Anda dilindungi.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-1 Anda	Pelajari bagaimana data Anda dilindungi.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
Data-1 Anda	Pelajari bagaimana data Anda dilindungi.	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
Data-1 Anda	Pelajari bagaimana data Anda dilindungi.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-1 Anda	Pelajari bagaimana data Anda dilindungi.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-1 Anda	Pelajari bagaimana data Anda dilindungi.	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
Data-1 Anda	Pelajari bagaimana data Anda dilindungi.	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-1 Anda	Pelajari bagaimana data Anda dilindungi.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-1 Anda	Pelajari bagaimana data Anda dilindungi.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-1 Anda	Pelajari bagaimana data Anda dilindungi.	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Data-1 Anda	Pelajari bagaimana data Anda dilindungi.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-1 Anda	Pelajari bagaimana data Anda dilindungi.	s3- default-encryption -kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Data-1 Anda	Pelajari bagaimana data Anda dilindungi.	s3- bucket-ssl-request s-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-1 Anda	Pelajari bagaimana data Anda dilindungi.	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Data-1 Anda	Pelajari bagaimana data Anda dilindungi.	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-1 Anda	Pelajari bagaimana data Anda dilindungi.	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Data-1 Anda	Pelajari bagaimana data Anda dilindungi.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	opensearch-audit-logging-enabled	Pastikan pencatatan audit diaktifkan di domain OpenSearch Layanan Amazon Anda. Pencatatan audit memungkinkan Anda melacak aktivitas pengguna di OpenSearch domain Anda, termasuk keberhasilan dan kegagalan otentikasi, permintaan, perubahan indeks OpenSearch, dan kueri penelusuran yang masuk.
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredenal masuk dalam lingkungan proyek Codebuild . AWS Gunakan OAuth alih-alih token akses pribadi atau kredensyal masuk untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	s3- default-encryption -kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	sagemaker-endpoint -configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-n ode enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkrip si memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-2 Anda	Pelajari apa yang terjadi di jaringan Anda. kelola komponen jaringan dan perimeter, komponen host dan perangkat, data-at-rest serta aktivitas dalam perjalanan, dan perilaku pengguna.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfig urasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-3 Anda	Perlindungan sistem nama domain.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-4 Anda-4	Membangun backup otomatis reguler dan redundansi sistem kunci.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-4 Anda-4	Membangun backup otomatis reguler dan redundansi sistem kunci.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-4 Anda-4	Membangun backup otomatis reguler dan redundansi sistem kunci.	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-4 Anda-4	Membangun backup otomatis reguler dan redundansi sistem kunci.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-4 Anda-4	Membangun backup otomatis reguler dan redundansi sistem kunci.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-4 Anda-4	Membangun backup otomatis reguler dan redundansi sistem kunci.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-4 Anda-4	Membangun backup otomatis reguler dan redundansi sistem kunci.	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-4 Anda-4	Membangun backup otomatis reguler dan redundansi sistem kunci.	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-4 Anda-4	Membangun backup otomatis reguler dan redundansi sistem kunci.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-4 Anda-4	Membangun backup otomatis reguler dan redundansi sistem kunci.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-4 Anda-4	Membangun backup otomatis reguler dan redundansi sistem kunci.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-4 Anda-4	Membangun backup otomatis reguler dan redundansi sistem kunci.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-4 Anda-4	Membangun backup otomatis reguler dan redundansi sistem kunci.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-4 Anda-4	Membangun backup otomatis reguler dan redundansi sistem kunci.	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-4 Anda-4	Membangun backup otomatis reguler dan redundansi sistem kunci.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-4 Anda-4	Membangun backup otomatis reguler dan redundansi sistem kunci.	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-4 Anda-4	Membangun backup otomatis reguler dan redundansi sistem kunci.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data-4 Anda-4	Membangun backup otomatis reguler dan redundansi sistem kunci.	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.
Data Anda-5	Manfaatkan perlindun gan untuk cadangan, termasuk keamanan fisik, enkripsi, dan salinan offline.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data Anda-5	Manfaatkan perlindungan untuk cadangan, termasuk keamanan fisik, enkripsi, dan salinan offline.	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Respon Krisis Anda-2	Memimpin pengembangan struktur pelaporan internal untuk mendeteksi, berkomunikasi, dan menahan serangan.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Respon Krisis Anda-2	Memimpin pengembangan struktur pelaporan internal untuk mendeteksi, berkomunikasi, dan menahan serangan.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Booting Up: Hal yang Harus Dilakukan Pertama-1	Gunakan solusi cadangan yang secara otomatis dan terus menerus mencadangkan data penting dan konfigura si sistem.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Booting Up: Hal yang Harus Dilakukan Pertama-1	Gunakan solusi cadangan yang secara otomatis dan terus menerus mencadangkan data penting dan konfigura si sistem.	dynamodb-in-backup-plan	Untuk membantu proses pencadang an data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Booting Up: Hal yang Harus Dilakukan Pertama-1	Gunakan solusi cadangan yang secara otomatis dan terus menerus mencadangkan data penting dan konfigura si sistem.	dynamodb-pitr-enab led	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertah ankan cadangan dengan memastika n bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Booting Up: Hal yang Harus Dilakukan Pertama-1	Gunakan solusi cadangan yang secara otomatis dan terus menerus mencadangkan data penting dan konfigura si sistem.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Booting Up: Hal yang Harus Dilakukan Pertama-1	Gunakan solusi cadangan yang secara otomatis dan terus menerus mencadangkan data penting dan konfigurasi sistem.	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Booting Up: Hal yang Harus Dilakukan Pertama-1	Gunakan solusi cadangan yang secara otomatis dan terus menerus mencadangkan data penting dan konfigura si sistem.	efs-in-backup-plan	Untuk membantu proses pencadang an data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Booting Up: Hal yang Harus Dilakukan Pertama-1	Gunakan solusi cadangan yang secara otomatis dan terus menerus mencadangkan data penting dan konfigura si sistem.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Booting Up: Hal yang Harus Dilakukan Pertama-1	Gunakan solusi cadangan yang secara otomatis dan terus menerus mencadangkan data penting dan konfigura si sistem.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Booting Up: Hal yang Harus Dilakukan Pertama-1	Gunakan solusi cadangan yang secara otomatis dan terus menerus mencadangkan data penting dan konfigurasi sistem.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Booting Up: Hal yang Harus Dilakukan Pertama-1	Gunakan solusi cadangan yang secara otomatis dan terus menerus mencadangkan data penting dan konfigura si sistem.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Booting Up: Hal yang Harus Dilakukan Pertama-1	Gunakan solusi cadangan yang secara otomatis dan terus menerus mencadangkan data penting dan konfigura si sistem.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Booting Up: Hal yang Harus Dilakukan Pertama-1	Gunakan solusi cadangan yang secara otomatis dan terus menerus mencadangkan data penting dan konfigura si sistem.	aurora-resources-p rotected-by-rencana cadangan	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Booting Up: Hal yang Harus Dilakukan Pertama-1	Gunakan solusi cadangan yang secara otomatis dan terus menerus mencadangkan data penting dan konfigurasi sistem.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Booting Up: Hal yang Harus Dilakukan Pertama-1	Gunakan solusi cadangan yang secara otomatis dan terus menerus mencadangkan data penting dan konfigurasi sistem.	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Booting Up: Hal yang Harus Dilakukan Pertama-1	Gunakan solusi cadangan yang secara otomatis dan terus menerus mencadangkan data penting dan konfigura si sistem.	dynamodb-resources-protected-by-rencana cadangan	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Booting Up: Hal yang Harus Dilakukan Pertama-1	Gunakan solusi cadangan yang secara otomatis dan terus menerus mencadangkan data penting dan konfigura si sistem.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Booting Up: Hal yang Harus Dilakukan Pertama-1	Gunakan solusi cadangan yang secara otomatis dan terus menerus mencadangkan data penting dan konfigura si sistem.	fsx-resources-prot ected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Booting Up: Hal yang Harus Dilakukan Pertama-2	Memerlukan otentikasi multi-faktor (MFA) untuk mengakses sistem Anda kapan pun memungkinkan.MFA harus diminta dari semua pengguna, tetapi mulailah dengan pengguna akses istimewa, administratif, dan jarak jauh.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Booting Up: Hal yang Harus Dilakukan Pertama-2	Memerlukan otentikasi multi-faktor (MFA) untuk mengakses sistem Anda kapan pun memungkinkan.MFA harus diminta dari semua pengguna, tetapi mulailah dengan pengguna akses istimewa, administratif, dan jarak jauh.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Booting Up: Hal yang Harus Dilakukan Pertama-2	Memerlukan otentikasi multi-faktor (MFA) untuk mengakses sistem Anda kapan pun memungkinkan.MFA harus diminta dari semua pengguna, tetapi mulailah dengan pengguna akses istimewa, administratif, dan jarak jauh.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Booting Up: Hal yang Harus Dilakukan Pertama-2	Memerlukan otentikasi multi-faktor (MFA) untuk mengakses sistem Anda kapan pun memungkinkan.MFA harus diminta dari semua pengguna, tetapi mulailah dengan pengguna akses istimewa, administratif, dan jarak jauh.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Booting Up: Hal yang Harus Dilakukan Pertama-3	Aktifkan pembaruan otomatis bila memungkinkan. Ganti sistem operasi, aplikasi, dan perangkat keras yang tidak didukung. Uji dan gunakan tambalan dengan cepat.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Booting Up: Hal yang Harus Dilakukan Pertama-3	Aktifkan pembaruan otomatis bila memungkinkan. Ganti sistem operasi, aplikasi, dan perangkat keras yang tidak didukung. Uji dan gunakan tambalan dengan cepat.	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relational Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Booting Up: Hal yang Harus Dilakukan Pertama-3	Aktifkan pembaruan otomatis bila memungkinkan. Ganti sistem operasi, aplikasi, dan perangkat keras yang tidak didukung. Uji dan gunakan tambalan dengan cepat.	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Booting Up: Hal yang Harus Dilakukan Pertama-3	Aktifkan pembaruan otomatis bila memungkinkan. Ganti sistem operasi, aplikasi, dan perangkat keras yang tidak didukung. Uji dan gunakan tambalan dengan cepat.	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

Templat

Template ini tersedia di GitHub: Praktik Terbaik Operasional untuk CISA Cyber Essentials.

Praktik Terbaik Operasional untuk Layanan Informasi Peradilan Pidana (CJIS)

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara Persyaratan Kepatuhan Layanan Informasi Peradilan Pidana (CJIS) dan aturan AWS Config yang dikelola. Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan berhubungan dengan satu atau beberapa kontrol CJIS. Kontrol CJIS dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.2	Pelatihan Kesadaran Keamanan	security-awareness -program-exists (Pemeriksaan Proses)	Membangun dan memelihara program kesadaran keamanan untuk organisas i Anda. Program kesadaran keamanan mendidik karyawan tentang cara melindungi organisas i mereka dari berbagai pelanggaran atau insiden keamanan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.3	Tanggapan Insiden	response-plan-exists-maintained (Pemeriksaan Proses)	Memastikan rencana respons insiden dibuat, dipelihara, dan didistribusikan kepada personel yang bertanggung jawab. Memiliki rencana respons yang diperbarui dan didokumentasikan secara formal dapat membantu memastikan personel respons memahami peran, tanggung jawab, dan proses yang harus diikuti selama insiden.
5.3	Tanggapan Insiden	response-plan-tested (Pemeriksaan Proses)	Pastikan respon Insiden dan rencana pemulihan diuji. Ini dapat membantu dalam memahami apakah rencana Anda akan efektif selama insiden dan jika ada celah atau pembaruan yang perlu ditangani.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.4	Audit dan Akuntabilitas	audit-log-policy-exists (Pemeriksaan proses)	Menetapkan dan memelihara kebijakan manajemen log audit yang menentukan persyaratan pencatatan organisasi Anda. Ini termasuk, namun tidak terbatas pada, peninjauan dan retensi log audit.
5.4.1	Acara dan Konten yang Dapat Diaudit (Sistem Informasi)	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
5.4.1	Acara dan Konten yang Dapat Diaudit (Sistem Informasi)	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.4.1	Acara dan Konten yang Dapat Diaudit (Sistem Informasi)	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.4.1	Acara dan Konten yang Dapat Diaudit (Sistem Informasi)	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus, atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.4.1	Acara dan Konten yang Dapat Diaudit (Sistem Informasi)	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi terperinci tentang proyek build Anda.
5.4.1	Acara dan Konten yang Dapat Diaudit (Sistem Informasi)	codebuild-project-s3-log-terenkripsi	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk AWS CodeBuild log Anda yang disimpan di Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.4.1	Acara dan Konten yang Dapat Diaudit (Sistem Informasi)	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.
5.4.1	Acara dan Konten yang Dapat Diaudit (Sistem Informasi)	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.4.1	Acara dan Konten yang Dapat Diaudit (Sistem Informasi)	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.4.1	Acara dan Konten yang Dapat Diaudit (Sistem Informasi)	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.4.1	Acara dan Konten yang Dapat Diaudit (Sistem Informasi)	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.4.1	Acara dan Konten yang Dapat Diaudit (Sistem Informasi)	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.4.1	Acara dan Konten yang Dapat Diaudit (Sistem Informasi)	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.4.1	Acara dan Konten yang Dapat Diaudit (Sistem Informasi)	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatata n AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.4.1	Acara dan Konten yang Dapat Diaudit (Sistem Informasi)	opensearch-audit-logging-enabled	Pastikan pencatatan audit diaktifkan di domain OpenSearch Layanan Amazon Anda. Pencatatan audit memungkinkan Anda melacak aktivitas pengguna di OpenSearch domain Anda, termasuk keberhasilan dan kegagalan otentikasi, permintaan, perubahan indeks OpenSearch, dan kueri penelusuran yang masuk.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.4.1	Acara dan Konten yang Dapat Diaudit (Sistem Informasi)	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.
5.4.1	Acara dan Konten yang Dapat Diaudit (Sistem Informasi)	redshift-audit-logging-enabled	Untuk menangkap informasi tentang koneksi dan aktivitas pengguna di klaster Amazon Redshift, pastikan pencatatan audit diaktifkan.
5.4.5	Perlindungan Informasi Audit	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.4.5	Perlindungan Informasi Audit	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus, atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.4.5	Perlindungan Informasi Audit	codebuild-project-s3-log-terenkripsi	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk AWS CodeBuild log Anda yang disimpan di Amazon S3.
5.4.6	Retensi Catatan Audit	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.4.6	Retensi Catatan Audit	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.5.2	Penegakan Akses	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.5.2	Penegakan Akses	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.5.2	Penegakan Akses	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
5.5.2	Penegakan Akses	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.5.2	Penegakan Akses	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (nilai CJIS: false), RequireLowercaseCharacters (nilai CJIS: false), (nilai CJIS: false), RequireSymbols (nilai CJIS: false), RequireNumbers (nilai CJIS: 8), MinimumPasswordLength (Nilai CJIS: 10), dan PasswordReusePreve

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			ntion (Nilai CJIS: 90) untuk Kebijakan Kata Sandi IAM Anda. MaxPasswordAge Nilai aktual harus mencerminkan kebijakan organisasi Anda.
5.5.2	Penegakan Akses	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.5.2	Penegakan Akses	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.5.2	Penegakan Akses	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.5.2	Penegakan Akses	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.5.2	Penegakan Akses	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.5.2	Penegakan Akses	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsageUsia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.5.2	Penegakan Akses	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.5.2	Penegakan Akses	rds-instance-iam-authentication-diaktifkan	Pastikan autentikasi AWS Identity and Access Management (IAM) diaktifkan pada instans Amazon Relational Database Service (Amazon RDS) untuk mengontrol akses ke sistem dan aset. Ini memberlakukan lalu lintas jaringan ke dan dari database yang akan dienkripsi menggunakan Secure Sockets Layer (SSL). Anda tidak diharuskan untuk menyimpan kredensyal pengguna dalam database, karena otentikasi dikelola secara eksternal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.5.2	Penegakan Akses	s3- bucket-acl-prohibited	Aturan ini memeriksa untuk melihat apakah Daftar Kontrol Akses (ACLs) digunakan untuk kontrol akses di Bucket Amazon S3. ACLs adalah mekanisme kontrol akses lama untuk bucket Amazon S3 yang AWS mendahului Identity and Access Management (IAM). Sebagai gantinya ACLs, ini adalah praktik terbaik untuk menggunakan kebijakan IAM atau kebijakan bucket S3 untuk mengelola akses ke bucket S3 Anda dengan lebih mudah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.5.2.1	Keistimewaan Terkecil	codebuild-project-environment-privileged-periksa	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan lingkungan CodeBuild proyek Amazon Anda tidak mengaktifkan mode istimewa. Pengaturan ini harus dinonaktifkan untuk mencegah akses yang tidak diinginkan ke Docker APIs serta perangkat keras yang mendasari container .™
5.5.2.1	Keistimewaan Terkecil	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.5.2.1	Keistimewaan Terkecil	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.5.2.1	Keistimewaan Terkecil	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
5.5.2.1	Keistimewaan Terkecil	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.5.2.1	Keistimewaan Terkecil	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.5.2.1	Keistimewaan Terkecil	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
5.5.2.1	Keistimewaan Terkecil	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.5.2.1	Keistimewaan Terkecil	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsageUsia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.5.2.1	Keistimewaan Terkecil	ecs-containers-non privileged	Untuk membantu menerapkan prinsip hak istimewa paling rendah, definisi tugas Amazon Elastic Container Service (Amazon ECS) seharusnya tidak mengaktifkan hak istimewa yang ditinggikan. Ketika parameter ini benar, wadah diberikan hak istimewa yang ditinggikan pada instance wadah host (mirip dengan pengguna root).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.5.2.1	Keistimewaan Terkecil	ecs-containers-readonly-access	Mengaktifkan akses baca saja ke wadah Amazon Elastic Container Service (ECS) dapat membantu mematuhi prinsip hak istimewa yang paling rendah. Opsi ini dapat mengurangi vektor serangan karena sistem file instance kontainer tidak dapat dimodifikasi kecuali jika memiliki izin baca-tulis eksplisit.™
5.5.2.1	Keistimewaan Terkecil	ecs-task-definition-nonroot-pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan bahwa pengguna non-root ditunjuk untuk mengakses definisi tugas Amazon Elastic Container Service (Amazon ECS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.5.2.1	Keistimewaan Terkecil	efs-access-point-enforce-identitas pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan penegakan pengguna diaktifkan untuk Amazon Elastic File System (Amazon EFS) Anda. Saat diaktifkan, Amazon EFS mengganti kan pengguna dan grup klien NFS IDs dengan identitas yang dikonfigurasi pada titik akses untuk semua operasi sistem file dan hanya memberika n akses ke identitas pengguna yang diberlakukan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.5.2.1	Keistimewaan Terkecil	secretsmanager-secret-unused	Jika kredensyal yang tidak digunakan ada di AWS Secrets Manager, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini memungkinkan Anda untuk menetapkan nilai ke unusedFor Days (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.5.6	Akses Jarak Jauh	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.5.6	Akses Jarak Jauh	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.6.2.1.1	Kata sandi	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (nilai CJIS: false), RequireLowercaseCharacters (nilai CJIS: false), (nilai CJIS: false), RequireSymbols (nilai CJIS: false), RequireNumbers (nilai CJIS: 8), MinimumPasswordLength (Nilai CJIS: 10), dan PasswordReusePreve

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			ntion (Nilai CJIS: 90) untuk Kebijakan Kata Sandi IAM Anda. MaxPasswo rdAge Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.6.2.2	Otentikasi Tingkat Lanjut	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.6.2.2	Otentikasi Tingkat Lanjut	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.6.2.2	Otentikasi Tingkat Lanjut	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.6.2.2	Otentikasi Tingkat Lanjut	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.6.2.2	Otentikasi Tingkat Lanjut	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.6.3.1	Manajemen Identifier	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsageUsia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.7.1.1	Fungsionalitas Paling Sedikit	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
5.7.1.1	Fungsionalitas Paling Sedikit	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.7.1.1	Fungsionalitas Paling Sedikit	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
5.7.1.1	Fungsionalitas Paling Sedikit	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.7.1.1	Fungsionalitas Paling Sedikit	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
5.7.1.1	Fungsionalitas Paling Sedikit	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.7.1.1	Fungsionalitas Paling Sedikit	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.7.1.1	Fungsionalitas Paling Sedikit	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.7.1.1	Fungsionalitas Paling Sedikit	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsageUsia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.7.1.1	Fungsionalitas Paling Sedikit	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.7.1.1	Fungsionalitas Paling Sedikit	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.7.1.1	Fungsionalitas Paling Sedikit	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.7.1.1	Fungsionalitas Paling Sedikit	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.7.1.1	Fungsionalitas Paling Sedikit	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
5.7.1.1	Fungsionalitas Paling Sedikit	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.7.1.1	Fungsionalitas Paling Sedikit	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
5.7.1.1	Fungsionalitas Paling Sedikit	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.7.1.1	Fungsionalitas Paling Sedikit	s3- account-level-publ ic-access -blok-per iodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.7.1.1	Fungsionalitas Paling Sedikit	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
5.7.1.1	Fungsionalitas Paling Sedikit	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.7.1.1	Fungsionalitas Paling Sedikit	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.7.1.1	Fungsionalitas Paling Sedikit	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.7.1.1	Fungsionalitas Paling Sedikit	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.7.1.1	Fungsionalitas Paling Sedikit	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.7.1.1	Fungsionalitas Paling Sedikit	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.7.1.1	Fungsionalitas Paling Sedikit	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.7.1.1	Fungsionalitas Paling Sedikit	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.7.1.1	Fungsionalitas Paling Sedikit	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
5.10	Perlindungan Sistem dan Komunikasi dan Integritas Informasi	alb-http-drop-invalid-Header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10	Perlindungan Sistem dan Komunikasi dan Integritas Informasi	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10	Perlindungan Sistem dan Komunikasi dan Integritas Informasi	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindungi nya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10	Perlindungan Sistem dan Komunikasi dan Integritas Informasi	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
5.10	Perlindungan Sistem dan Komunikasi dan Integritas Informasi	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10	Perlindungan Sistem dan Komunikasi dan Integritas Informasi	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10	Perlindungan Sistem dan Komunikasi dan Integritas Informasi	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10	Perlindungan Sistem dan Komunikasi dan Integritas Informasi	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10	Perlindungan Sistem dan Komunikasi dan Integritas Informasi	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10	Perlindungan Sistem dan Komunikasi dan Integritas Informasi	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10	Perlindungan Sistem dan Komunikasi dan Integritas Informasi	s3- bucket-acl-prohibited	Aturan ini memeriksa untuk melihat apakah Daftar Kontrol Akses (ACLs) digunakan untuk kontrol akses di Bucket Amazon S3. ACLs adalah mekanisme kontrol akses lama untuk bucket Amazon S3 yang AWS mendahului Identity and Access Management (IAM). Sebagai gantinya ACLs, ini adalah praktik terbaik untuk menggunakan kebijakan IAM atau kebijakan bucket S3 untuk mengelola akses ke bucket S3 Anda dengan lebih mudah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10	Perlindungan Sistem dan Komunikasi dan Integritas Informasi	vpc-network-acl-unused-periksa	Aturan ini memastikan bahwa daftar kontrol akses jaringan Amazon Virtual Private Cloud (VPC) sedang digunakan. Pemantauan untuk daftar kontrol akses jaringan yang tidak digunakan dapat membantu inventaris dan pengelolaan lingkungan Anda yang akurat.
5.10	Perlindungan Sistem dan Komunikasi dan Integritas Informasi	waf-regional-webacl-not-kosong	Web ACL yang dilampirkan ke AWS WAF dapat berisi kumpulan aturan dan kelompok aturan untuk memeriksa dan mengontrol permintaan web. Jika ACL Web kosong, lalu lintas web lewat tanpa terdeteksi atau ditindaklanjuti oleh WAF.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1	Penegakan Arus Informasi	alb-http-drop-invalid-Header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
5.10.1	Penegakan Arus Informasi	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1	Penegakan Arus Informasi	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
5.10.1	Penegakan Arus Informasi	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1	Penegakan Arus Informasi	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1	Penegakan Arus Informasi	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1	Penegakan Arus Informasi	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1	Penegakan Arus Informasi	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1	Penegakan Arus Informasi	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
5.10.1	Penegakan Arus Informasi	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1	Penegakan Arus Informasi	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
5.10.1	Penegakan Arus Informasi	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1	Penegakan Arus Informasi	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
5.10.1	Penegakan Arus Informasi	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1	Penegakan Arus Informasi	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.
5.10.1	Penegakan Arus Informasi	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1	Penegakan Arus Informasi	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1	Penegakan Arus Informasi	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1	Penegakan Arus Informasi	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
5.10.1	Penegakan Arus Informasi	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1	Penegakan Arus Informasi	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
5.10.1	Penegakan Arus Informasi	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1	Penegakan Arus Informasi	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1	Penegakan Arus Informasi	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
5.10.1	Penegakan Arus Informasi	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1	Penegakan Arus Informasi	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1	Penegakan Arus Informasi	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1	Penegakan Arus Informasi	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1.1	Perlindungan Batas	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1.1	Perlindungan Batas	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1.1	Perlindungan Batas	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindunginya dari serangan berbahaya
5.10.1.1	Perlindungan Batas	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1.1	Perlindungan Batas	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1.1	Perlindungan Batas	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1.1	Perlindungan Batas	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
5.10.1.1	Perlindungan Batas	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1.1	Perlindungan Batas	waf-regional-rule-not-kosong	Pastikan AWS WAF Anda memiliki aturan yang tidak kosong. Aturan tanpa kondisi dapat mengakibatkan perilaku yang tidak diinginkan.
5.10.1.1	Perlindungan Batas	waf-regional-rulegroup-not-kosong	Pastikan AWS WAF Anda memiliki grup aturan yang tidak kosong. Grup aturan yang kosong dapat mengakibatkan perilaku yang tidak diinginkan.
5.10.1.1	Perlindungan Batas	waf-regional-webacl-not-kosong	Web ACL yang dilampirkan ke AWS WAF dapat berisi kumpulan aturan dan kelompok aturan untuk memeriksa dan mengontrol permintaan web. Jika ACL Web kosong, lalu lintas web lewat tanpa terdeteksi atau ditindaklanjuti oleh WAF.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1.2	Enkripsi	alb-http-drop-invalid-Header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
5.10.1.2	Enkripsi	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1.2	Enkripsi	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
5.10.1.2	Enkripsi	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomen dasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaa n enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1.2	Enkripsi	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
5.10.1.2	Enkripsi	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrai l jejak Anda.
5.10.1.2	Enkripsi	codebuild-project-artifact-encryption	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk AWS CodeBuild artefak Anda.
5.10.1.2	Enkripsi	codebuild-project-s3-log-terenkripsi	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk AWS CodeBuild log Anda yang disimpan di Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1.2	Enkripsi	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
5.10.1.2	Enkripsi	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1.2	Enkripsi	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
5.10.1.2	Enkripsi	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1.2	Enkripsi	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1.2	Enkripsi	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1.2	Enkripsi	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
5.10.1.2	Enkripsi	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1.2	Enkripsi	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
5.10.1.2	Enkripsi	kinesis-stream-encrypted	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.
5.10.1.2	Enkripsi	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1.2	Enkripsi	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1.2	Enkripsi	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1.2	Enkripsi	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
5.10.1.2	Enkripsi	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1.2	Enkripsi	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
5.10.1.2	Enkripsi	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1.2	Enkripsi	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
5.10.1.2	Enkripsi	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1.2	Enkripsi	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
5.10.1.2	Enkripsi	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1.2	Enkripsi	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
5.10.1.2	Enkripsi	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1.2	Enkripsi	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
5.10.1.2	Enkripsi	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1.3	Alat dan Teknik Deteksi Intrusi	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1.3	Alat dan Teknik Deteksi Intrusi	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.1.3	Alat dan Teknik Deteksi Intrusi	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.4.1	Manajemen Patch	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.4.1	Manajemen Patch	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.4.1	Manajemen Patch	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.4.1	Manajemen Patch	ecs-fargate-latest-platform-versi	Pembaruan dan tambalan keamanan diterapkan secara otomatis untuk tugas Fargate AWS Anda. Jika ditemukan masalah keamanan yang memengaru hi versi platform AWS Fargate, AWS tambal versi platform. Untuk membantu pengelolaan tambalan tugas Amazon Elastic Container Service (ECS) yang menjalank an AWS Fargate, perbarui tugas mandiri layanan Anda untuk menggunakan versi platform terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.4.1	Manajemen Patch	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.4.4	Peringatan dan Penasihat Keamanan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.4.4	Peringatan dan Penasihat Keamanan	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.10.4.4	Peringatan dan Penasihat Keamanan	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk CJIS.

Praktik Terbaik Operasional untuk CMMC 2.0 Level 1

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS

Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara aturan Cybersecurity Maturity Model Certification (CMMC) 2.0 Level 1 dan managed AWS Config. Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau beberapa kontrol CMMC 2.0 Level 1. Kontrol CMMC 2.0 Level 1 dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			kebijakan organisasi Anda.
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifka n untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredensyal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredensyal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensyal masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensyal masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	secretsmanager-rotation-enabled-check	Aturan ini memastikan AWS rahasia Secrets Manager telah diaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	secretsmanager-scheduled-rotation-success-periksa	Aturan ini memastikan bahwa AWS rahasia Secrets Manager telah berhasil diputar sesuai dengan jadwal rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode di mana rahasia aktif, dan berpotensi mengurangi dampak bisnis jika dikompromikan.
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSear ch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerluka n gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredensyal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredensyal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensyal masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensyal masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
AC.L1-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC.L1-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
AC.L1-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
AC.L1-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
AC.L1-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
AC.L1-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
AC.L1-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L1-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L1-3.5.1	Identifikasi pengguna sistem informasi, proses yang bertindak atas nama pengguna, atau perangkat.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
IA.L1-3.5.1	Identifikasi pengguna sistem informasi, proses yang bertindak atas nama pengguna, atau perangkat.	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L1-3.5.1	Identifikasi pengguna sistem informasi, proses yang bertindak atas nama pengguna, atau perangkat.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
IA.L1-3.5.1	Identifikasi pengguna sistem informasi, proses yang bertindak atas nama pengguna, atau perangkat.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L1-3.5.1	Identifikasi pengguna sistem informasi, proses yang bertindak atas nama pengguna, atau perangkat.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L1-3.5.1	Identifikasi pengguna sistem informasi, proses yang bertindak atas nama pengguna, atau perangkat.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L1-3.5.1	Identifikasi pengguna sistem informasi, proses yang bertindak atas nama pengguna, atau perangkat.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L1-3.5.1	Identifikasi pengguna sistem informasi, proses yang bertindak atas nama pengguna, atau perangkat.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L1-3.5.1	Identifikasi pengguna sistem informasi, proses yang bertindak atas nama pengguna, atau perangkat.	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatata n AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L1-3.5.2	Mengautentikasi (atau memverifi kasi) identitas pengguna, proses, atau perangkat tersebut, sebagai prasyarat untuk memungkinkan akses ke sistem informasi organisasi.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L1-3.5.2	Mengautentikasi (atau memverifikasi) identitas pengguna, proses, atau perangkat tersebut, sebagai prasyarat untuk memungkinkan akses ke sistem informasi organisasi.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L1-3.5.2	Mengautentikasi (atau memverifi kasi) identitas pengguna, proses, atau perangkat tersebut, sebagai prasyarat untuk memungkinkan akses ke sistem informasi organisasi.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastika n otentikasi multi-fak tor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindun gan ekstra di atas kredensyal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L1-3.5.2	Mengautentikasi (atau memverifi kasi) identitas pengguna, proses, atau perangkat tersebut, sebagai prasyarat untuk memungkinkan akses ke sistem informasi organisasi.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredensyal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L1-3.5.2	Mengautentikasi (atau memverifikasi) identitas pengguna, proses, atau perangkat tersebut, sebagai prasyarat untuk memungkinkan akses ke sistem informasi organisasi.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensyal masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L1-3.5.2	Mengautentikasi (atau memverifikasi) identitas pengguna, proses, atau perangkat tersebut, sebagai prasyarat untuk memungkinkan akses ke sistem informasi organisasi.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensyal masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	alb-http-drop-invalid-header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindunginya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigurasi ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L1-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L1-3.14.1	Identifikasi, laporkan, dan perbaiki kekurangan sistem informasi dan informasi secara tepat waktu.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L1-3.14.1	Identifikasi, laporkan, dan perbaiki kekurangan sistem informasi dan informasi secara tepat waktu.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L1-3.14.1	Identifikasi, laporkan, dan perbaiki kekurangan sistem informasi dan informasi secara tepat waktu.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L1-3.14.2	Memberikan perlindungan dari kode berbahaya di lokasi yang sesuai dalam sistem informasi organisasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L1-3.14.5	Lakukan pemindaian berkala sistem informasi dan pemindaian file secara real-time dari sumber eksternal saat file diunduh, dibuka, atau dieksekusi.	ecr-private-image-scanning-diaktifkan	Pemindaian gambar Amazon Elastic Container Repository (ECR) membantu mengidentifikasi kerentanan perangkat lunak dalam gambar kontainer Anda. Mengaktifkan pemindaian gambar pada repositori ECR menambahkan lapisan verifikasi untuk integritas dan keamanan gambar yang disimpan.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk CMMC 2.0 Level 1.

Praktik Terbaik Operasional untuk CMMC 2.0 Level 2

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara aturan Cybersecurity Maturity Model Certification (CMMC) 2.0 Level 2 dan managed AWS Config. Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau beberapa kontrol CMMC 2.0 Level 2. Kontrol CMMC 2.0

Level 2 dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	berwenang, atau perangkat (termasuk sistem informasi lainnya).		dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	secretsmanager-rotation-enabled-check	Aturan ini memastikan AWS rahasia Secrets Manager telah diaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan.
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	secretsmanager-scheduled-rotation-success-periksa	Aturan ini memastikan bahwa AWS rahasia Secrets Manager telah berhasil diputar sesuai dengan jadwal rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode di mana rahasia aktif, dan berpotensi mengurangi dampak bisnis jika dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.1	Batasi akses sistem informasi ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, atau perangkat (termasuk sistem informasi lainnya).	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSear ch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerluka n gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.2	Batasi akses sistem informasi ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk dijalankan.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
AC.L2-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC.L2-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
AC.L2-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
AC.L2-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
AC.L2-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
AC.L2-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem informasi eksternal.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindungi nya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
AC.L2-3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC.L2-3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
AC.L2-3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
AC.L2-3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
AC.L2-3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC.L2-3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
AC.L2-3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
AC.L2-3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.4	Pisahkan tugas individu untuk mengurangi risiko aktivitas jahat tanpa kolusi.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.4	Pisahkan tugas individu untuk mengurangi risiko aktivitas jahat tanpa kolusi.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
AC.L2-3.1.4	Pisahkan tugas individu untuk mengurangi risiko aktivitas jahat tanpa kolusi.	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.4	Pisahkan tugas individu untuk mengurangi risiko aktivitas jahat tanpa kolusi.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.4	Pisahkan tugas individu untuk mengurangi risiko aktivitas jahat tanpa kolusi.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.4	Pisahkan tugas individu untuk mengurangi risiko aktivitas jahat tanpa kolusi.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
AC.L2-3.1.4	Pisahkan tugas individu untuk mengurangi risiko aktivitas jahat tanpa kolusi.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.4	Pisahkan tugas individu untuk mengurangi risiko aktivitas jahat tanpa kolusi.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.4	Pisahkan tugas individu untuk mengurangi risiko aktivitas jahat tanpa kolusi.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.4	Pisahkan tugas individu untuk mengurangi risiko aktivitas jahat tanpa kolusi.	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs
AC.L2-3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC.L2-3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC.L2-3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSear ch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerluka n gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
AC.L2-3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
AC.L2-3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
AC.L2-3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
AC.L2-3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
AC.L2-3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs
AC.L2-3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
AC.L2-3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.6	Gunakan akun atau peran yang tidak memiliki hak istimewa saat mengakses fungsi non-keamanan.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.6	Gunakan akun atau peran yang tidak memiliki hak istimewa saat mengakses fungsi non-keamanan.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
AC.L2-3.1.6	Gunakan akun atau peran yang tidak memiliki hak istimewa saat mengakses fungsi non-keamanan.	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.6	Gunakan akun atau peran yang tidak memiliki hak istimewa saat mengakses fungsi non-keamanan.	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
AC.L2-3.1.6	Gunakan akun atau peran yang tidak memiliki hak istimewa saat mengakses fungsi non-keamanan.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.6	Gunakan akun atau peran yang tidak memiliki hak istimewa saat mengakses fungsi non-keamanan.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.6	Gunakan akun atau peran yang tidak memiliki hak istimewa saat mengakses fungsi non-keamanan.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
AC.L2-3.1.6	Gunakan akun atau peran yang tidak memiliki hak istimewa saat mengakses fungsi non-keamanan.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.6	Gunakan akun atau peran yang tidak memiliki hak istimewa saat mengakses fungsi non-keamanan.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.6	Gunakan akun atau peran yang tidak memiliki hak istimewa saat mengakses fungsi non-keamanan.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.
AC.L2-3.1.7	Mencegah pengguna yang tidak memiliki hak istimewa mengeksekusi fungsi istimewa dan menangkap eksekusi fungsi tersebut di log audit.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.7	Mencegah pengguna yang tidak memiliki hak istimewa mengeksekusi fungsi istimewa dan menangkap eksekusi fungsi tersebut di log audit.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
AC.L2-3.1.7	Mencegah pengguna yang tidak memiliki hak istimewa mengeksekusi fungsi istimewa dan menangkap eksekusi fungsi tersebut di log audit.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.7	Mencegah pengguna yang tidak memiliki hak istimewa mengeksekusi fungsi istimewa dan menangkap eksekusi fungsi tersebut di log audit.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.7	Mencegah pengguna yang tidak memiliki hak istimewa mengeksekusi fungsi istimewa dan menangkap eksekusi fungsi tersebut di log audit.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.7	Mencegah pengguna yang tidak memiliki hak istimewa mengeksekusi fungsi istimewa dan menangkap eksekusi fungsi tersebut di log audit.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.7	Mencegah pengguna yang tidak memiliki hak istimewa mengeksekusi fungsi istimewa dan menangkap eksekusi fungsi tersebut di log audit.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
AC.L2-3.1.7	Mencegah pengguna yang tidak memiliki hak istimewa mengeksekusi fungsi istimewa dan menangkap eksekusi fungsi tersebut di log audit.	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.7	Mencegah pengguna yang tidak memiliki hak istimewa mengeksekusi fungsi istimewa dan menangkap eksekusi fungsi tersebut di log audit.	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
AC.L2-3.1.7	Mencegah pengguna yang tidak memiliki hak istimewa mengeksekusi fungsi istimewa dan menangkap eksekusi fungsi tersebut di log audit.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.7	Mencegah pengguna yang tidak memiliki hak istimewa mengeksekusi fungsi istimewa dan menangkap eksekusi fungsi tersebut di log audit.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.7	Mencegah pengguna yang tidak memiliki hak istimewa mengeksekusi fungsi istimewa dan menangkap eksekusi fungsi tersebut di log audit.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
AC.L2-3.1.7	Mencegah pengguna yang tidak memiliki hak istimewa mengeksekusi fungsi istimewa dan menangkap eksekusi fungsi tersebut di log audit.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.7	Mencegah pengguna yang tidak memiliki hak istimewa mengeksekusi fungsi istimewa dan menangkap eksekusi fungsi tersebut di log audit.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.7	Mencegah pengguna yang tidak memiliki hak istimewa mengeksekusi fungsi istimewa dan menangkap eksekusi fungsi tersebut di log audit.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.7	Mencegah pengguna yang tidak memiliki hak istimewa mengeksekusi fungsi istimewa dan menangkap eksekusi fungsi tersebut di log audit.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.7	Mencegah pengguna yang tidak memiliki hak istimewa mengeksekusi fungsi istimewa dan menangkap eksekusi fungsi tersebut di log audit.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.7	Mencegah pengguna yang tidak memiliki hak istimewa mengeksekusi fungsi istimewa dan menangkap eksekusi fungsi tersebut di log audit.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.7	Mencegah pengguna yang tidak memiliki hak istimewa mengeksekusi fungsi istimewa dan menangkap eksekusi fungsi tersebut di log audit.	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.12	Pantau dan kendalikan sesi akses jarak jauh.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.12	Pantau dan kendalikan sesi akses jarak jauh.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
AC.L2-3.1.12	Pantau dan kendalikan sesi akses jarak jauh.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.12	Pantau dan kendalikan sesi akses jarak jauh.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.13	Gunakan mekanisme kriptografi untuk melindungi kerahasiaan sesi akses jarak jauh.	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
AC.L2-3.1.13	Gunakan mekanisme kriptografi untuk melindungi kerahasiaan sesi akses jarak jauh.	alb-http-to-https-pemeriksaan-pengalihan	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.13	Gunakan mekanisme kriptografi untuk melindungi kerahasiaan sesi akses jarak jauh.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.
AC.L2-3.1.13	Gunakan mekanisme kriptografi untuk melindungi kerahasiaan sesi akses jarak jauh.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.13	Gunakan mekanisme kriptografi untuk melindungi kerahasiaan sesi akses jarak jauh.	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.13	Gunakan mekanisme kriptografi untuk melindungi kerahasia an sesi akses jarak jauh.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
AC.L2-3.1.13	Gunakan mekanisme kriptografi untuk melindungi kerahasia an sesi akses jarak jauh.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.13	Gunakan mekanisme kriptografi untuk melindungi kerahasia an sesi akses jarak jauh.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
AC.L2-3.1.13	Gunakan mekanisme kriptografi untuk melindungi kerahasia an sesi akses jarak jauh.	s3- bucket-ssl-request s-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC.L2-3.1.13	Gunakan mekanisme kriptografi untuk melindungi kerahasiaan sesi akses jarak jauh.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
AU.L2-3.3.1	Membuat dan menyimpan log dan catatan audit sistem sejauh yang diperlukan untuk memungkinkan pemantauan, analisis, investigasi, dan pelaporan aktivitas sistem yang melanggar hukum atau tidak sah.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU.L2-3.3.1	Membuat dan menyimpan log dan catatan audit sistem sejauh yang diperlukan untuk memungkinkan pemantauan, analisis, investigasi, dan pelaporan aktivitas sistem yang melanggar hukum atau tidak sah.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
AU.L2-3.3.1	Membuat dan menyimpan log dan catatan audit sistem sejauh yang diperlukan untuk memungkinkan pemantauan, analisis, investigasi, dan pelaporan aktivitas sistem yang melanggar hukum atau tidak sah.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU.L2-3.3.1	Membuat dan menyimpan log dan catatan audit sistem sejauh yang diperlukan untuk memungkinkan pemantauan, analisis, investigasi, dan pelaporan aktivitas sistem yang melanggar hukum atau tidak sah.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU.L2-3.3.1	Membuat dan menyimpan log dan catatan audit sistem sejauh yang diperlukan untuk memungkinkan pemantauan, analisis, investigasi, dan pelaporan aktivitas sistem yang melanggar hukum atau tidak sah.	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU.L2-3.3.1	Membuat dan menyimpan log dan catatan audit sistem sejauh yang diperlukan untuk memungkinkan pemantauan, analisis, investigasi, dan pelaporan aktivitas sistem yang melanggar hukum atau tidak sah.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU.L2-3.3.1	Membuat dan menyimpan log dan catatan audit sistem sejauh yang diperlukan untuk memungkinkan pemantauan, analisis, investigasi, dan pelaporan aktivitas sistem yang melanggar hukum atau tidak sah.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU.L2-3.3.1	Membuat dan menyimpan log dan catatan audit sistem sejauh yang diperlukan untuk memungkinkan pemantauan, analisis, investigasi, dan pelaporan aktivitas sistem yang melanggar hukum atau tidak sah.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU.L2-3.3.1	Membuat dan menyimpan log dan catatan audit sistem sejauh yang diperlukan untuk memungkinkan pemantauan, analisis, investigasi, dan pelaporan aktivitas sistem yang melanggar hukum atau tidak sah.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU.L2-3.3.1	Membuat dan menyimpan log dan catatan audit sistem sejauh yang diperlukan untuk memungkinkan pemantauan, analisis, investigasi, dan pelaporan aktivitas sistem yang melanggar hukum atau tidak sah.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
MS.L2-3.3.2	Pastikan bahwa tindakan pengguna sistem individu dapat ditelusuri secara unik ke pengguna tersebut sehingga mereka dapat dimintakan pertanggungjawaban atas tindakan mereka.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
MS.L2-3.3.2	Pastikan bahwa tindakan pengguna sistem individu dapat ditelusuri secara unik ke pengguna tersebut sehingga mereka dapat dimintakan pertanggungjawaban atas tindakan mereka.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
MS.L2-3.3.2	Pastikan bahwa tindakan pengguna sistem individu dapat ditelusuri secara unik ke pengguna tersebut sehingga mereka dapat dimintakan pertanggungjawaban atas tindakan mereka.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
MS.L2-3.3.2	Pastikan bahwa tindakan pengguna sistem individu dapat ditelusuri secara unik ke pengguna tersebut sehingga mereka dapat dimintakan pertanggungjawaban atas tindakan mereka.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
MS.L2-3.3.2	Pastikan bahwa tindakan pengguna sistem individu dapat ditelusuri secara unik ke pengguna tersebut sehingga mereka dapat dimintakan pertanggungjawaban atas tindakan mereka.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
MS.L2-3.3.2	Pastikan bahwa tindakan pengguna sistem individu dapat ditelusuri secara unik ke pengguna tersebut sehingga mereka dapat dimintakan pertanggungjawaban atas tindakan mereka.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
MS.L2-3.3.2	Pastikan bahwa tindakan pengguna sistem individu dapat ditelusuri secara unik ke pengguna tersebut sehingga mereka dapat dimintakan pertanggungjawaban atas tindakan mereka.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
MS.L2-3.3.2	Pastikan bahwa tindakan pengguna sistem individu dapat ditelusuri secara unik ke pengguna tersebut sehingga mereka dapat dimintakan pertanggungjawaban atas tindakan mereka.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
MS.L2-3.3.2	Pastikan bahwa tindakan pengguna sistem individu dapat ditelusuri secara unik ke pengguna tersebut sehingga mereka dapat dimintakan pertanggungjawaban atas tindakan mereka.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU.L2-3.3.4	Peringatan jika terjadi kegagalan proses pencatatan audit.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU.L2-3.3.4	Peringatan jika terjadi kegagalan proses pencatatan audit.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
AU.L2-3.3.4	Peringatan jika terjadi kegagalan proses pencatatan audit.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU.L2-3.3.4	Peringatan jika terjadi kegagalan proses pencatatan audit.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU.L2-3.3.5	Mengkorelasikan proses peninjauan, analisis, dan pelaporan catatan audit untuk investigasi dan tanggapan terhadap indikasi aktivitas yang melanggar hukum, tidak sah, mencurigakan, atau tidak biasa.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU.L2-3.3.5	Mengkorelasikan proses peninjauan, analisis, dan pelaporan catatan audit untuk investigasi dan tanggapan terhadap indikasi aktivitas yang melanggar hukum, tidak sah, mencurigakan, atau tidak biasa.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
AU.L2-3.3.8	Lindungi informasi audit dan alat pencatatan audit dari akses, modifikasi, dan penghapusan yang tidak sah.	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU.L2-3.3.8	Lindungi informasi audit dan alat pencatatan audit dari akses, modifikasi, dan penghapusan yang tidak sah.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU.L2-3.3.8	Lindungi informasi audit dan alat pencatatan audit dari akses, modifikasi, dan penghapusan yang tidak sah.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU.L2-3.3.8	Lindungi informasi audit dan alat pencatatan audit dari akses, modifikasi, dan penghapusan yang tidak sah.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU.L2-3.3.8	Lindungi informasi audit dan alat pencatatan audit dari akses, modifikasi, dan penghapusan yang tidak sah.	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.
AU.L2-3.3.8	Lindungi informasi audit dan alat pencatatan audit dari akses, modifikasi, dan penghapusan yang tidak sah.	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU.L2-3.3.8	Lindungi informasi audit dan alat pencatatan audit dari akses, modifikasi, dan penghapusan yang tidak sah.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
AU.L2-3.3.8	Lindungi informasi audit dan alat pencatatan audit dari akses, modifikasi, dan penghapusan yang tidak sah.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU.L2-3.3.8	Lindungi informasi audit dan alat pencatatan audit dari akses, modifikasi, dan penghapusan yang tidak sah.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
AU.L2-3.3.8	Lindungi informasi audit dan alat pencatatan audit dari akses, modifikasi, dan penghapusan yang tidak sah.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU.L2-3.3.8	Lindungi informasi audit dan alat pencatatan audit dari akses, modifikasi, dan penghapusan yang tidak sah.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU.L2-3.3.8	Lindungi informasi audit dan alat pencatatan audit dari akses, modifikasi, dan penghapusan yang tidak sah.	s3- default-encryption -kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CA.L2-3.12.2	Mengembangkan dan melaksanakan rencana tindakan yang dirancang untuk memperbai ki kekurangan dan mengurangi atau menghilangkan kerentanan dalam sistem organisasi.	vuln-management-pl an-exists (Pemeriks aan Proses)	Pastikan rencana manajemen kerentana n dikembangkan dan diimplementasikan untuk memiliki proses yang ditentukan secara formal untuk mengatasi kerentana n di lingkungan Anda. Ini dapat mencakup alat manajemen kerentana n, irama pemindaian lingkungan, peran dan tanggung jawab.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
MS.L2-3.12.3	Pantau kontrol keamanan secara berkelanjutan untuk memastikan efektivitas kontrol yang berkelanjutan.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
MS.L2-3.12.3	Pantau kontrol keamanan secara berkelanjutan untuk memastikan efektivitas kontrol yang berkelanjutan.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
MS.L2-3.12.3	Pantau kontrol keamanan secara berkelanjutan untuk memastikan efektivit as kontrol yang berkelanjutan.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.1	Menetapkan dan memelihara konfigurasi dasar dan inventaris sistem organisasi (termasuk perangkat keras, perangkat lunak, firmware, dan dokumentasi) di seluruh siklus hidup pengembangan sistem masing-masing.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.1	Menetapkan dan memelihara konfigurasi dasar dan inventaris sistem organisasi (termasuk perangkat keras, perangkat lunak, firmware, dan dokumentasi) di seluruh siklus hidup pengembangan sistem masing-masing.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
CM.L2-3.4.1	Menetapkan dan memelihara konfigurasi dasar dan inventaris sistem organisasi (termasuk perangkat keras, perangkat lunak, firmware, dan dokumentasi) di seluruh siklus hidup pengembangan sistem masing-masing.	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.1	Menetapkan dan memelihara konfigurasi dasar dan inventaris sistem organisasi (termasuk perangkat keras, perangkat lunak, firmware, dan dokumentasi) di seluruh siklus hidup pengembangan sistem masing-masing.	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.
CM.L2-3.4.1	Menetapkan dan memelihara konfigurasi dasar dan inventaris sistem organisasi (termasuk perangkat keras, perangkat lunak, firmware, dan dokumentasi) di seluruh siklus hidup pengembangan sistem masing-masing.	terlampir eip	Aturan ini memastikan Elastic IPs dialokasikan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan. Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.2	Menetapkan dan menegakkan pengaturan konfigurasi keamanan untuk produk teknologi informasi yang digunakan dalam sistem organisasi.	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.
CM.L2-3.4.2	Menetapkan dan menegakkan pengaturan konfigurasi keamanan untuk produk teknologi informasi yang digunakan dalam sistem organisasi.	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.2	Menetapkan dan menegakkan pengaturan konfigurasi keamanan untuk produk teknologi informasi yang digunakan dalam sistem organisasi.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.2	Menetapkan dan menegakkan pengaturan konfigura si keamanan untuk produk teknologi informasi yang digunakan dalam sistem organisasi.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.2	Menetapkan dan menegakkan pengaturan konfigurasi keamanan untuk produk teknologi informasi yang digunakan dalam sistem organisasi.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.2	Menetapkan dan menegakkan pengaturan konfigurasi keamanan untuk produk teknologi informasi yang digunakan dalam sistem organisasi.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
CM.L2-3.4.2	Menetapkan dan menegakkan pengaturan konfigurasi keamanan untuk produk teknologi informasi yang digunakan dalam sistem organisasi.	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.2	Menetapkan dan menegakkan pengaturan konfigura si keamanan untuk produk teknologi informasi yang digunakan dalam sistem organisasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.2	Menetapkan dan menegakkan pengaturan konfigurasi keamanan untuk produk teknologi informasi yang digunakan dalam sistem organisasi.	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relational Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.2	Menetapkan dan menegakkan pengaturan konfigurasi keamanan untuk produk teknologi informasi yang digunakan dalam sistem organisasi.	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.2	Menetapkan dan menegakkan pengaturan konfigura si keamanan untuk produk teknologi informasi yang digunakan dalam sistem organisasi.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.3	Melacak, meninjau, menyetujui, atau tidak menyetuju i, dan mencatat perubahan pada sistem organisasi.	api-gw-execution-l ogging-diaktifkan	Pencatatan API Gateway menampilk an tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
CM.L2-3.4.3	Melacak, meninjau, menyetujui, atau tidak menyetuju i, dan mencatat perubahan pada sistem organisasi.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteks i aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.3	Melacak, meninjau, menyetujui, atau tidak menyetuju i, dan mencatat perubahan pada sistem organisasi.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
CM.L2-3.4.3	Melacak, meninjau, menyetujui, atau tidak menyetuju i, dan mencatat perubahan pada sistem organisasi.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.3	Melacak, meninjau, menyetujui, atau tidak menyetuju i, dan mencatat perubahan pada sistem organisasi.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.3	Melacak, meninjau, menyetujui, atau tidak menyetuju i, dan mencatat perubahan pada sistem organisasi.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventari s platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.3	Melacak, meninjau, menyetujui, atau tidak menyetuju i, dan mencatat perubahan pada sistem organisasi.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.3	Melacak, meninjau, menyetujui, atau tidak menyetuju i, dan mencatat perubahan pada sistem organisasi.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.3	Melacak, meninjau, menyetujui, atau tidak menyetuju i, dan mencatat perubahan pada sistem organisasi.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.3	Melacak, meninjau, menyetujui, atau tidak menyetuju i, dan mencatat perubahan pada sistem organisasi.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.3	Melacak, meninjau, menyetujui, atau tidak menyetuju i, dan mencatat perubahan pada sistem organisasi.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediak an metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinc i untuk permintaa n yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.3	Melacak, meninjau, menyetujui, atau tidak menyetuju i, dan mencatat perubahan pada sistem organisasi.	wafv2-logging-diak tifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatata n AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfig urasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
CM.L2-3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CM.L2-3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventari s platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfigurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSear ch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerluka n gateway internet, perangkat NAT, atau koneksi VPN.
CM.L2-3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfigurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
CM.L2-3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfigurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
CM.L2-3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
CM.L2-3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfigurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
CM.L2-3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
CM.L2-3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkin kan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspo s informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurk an ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/ 0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.7	Membatasi, menonaktifkan, atau mencegah penggunaan program, fungsi, port, protokol, dan layanan yang tidak penting.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
CM.L2-3.4.7	Membatasi, menonaktifkan, atau mencegah penggunaan program, fungsi, port, protokol, dan layanan yang tidak penting.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.7	Membatasi, menonaktifkan, atau mencegah penggunaan program, fungsi, port, protokol, dan layanan yang tidak penting.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CM.L2-3.4.7	Membatasi, menonaktifkan, atau mencegah penggunaan program, fungsi, port, protokol, dan layanan yang tidak penting.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.7	Membatasi, menonaktifkan, atau mencegah penggunaan program, fungsi, port, protokol, dan layanan yang tidak penting.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
CM.L2-3.4.7	Membatasi, menonaktifkan, atau mencegah penggunaan program, fungsi, port, protokol, dan layanan yang tidak penting.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.7	Membatasi, menonaktifkan, atau mencegah penggunaan program, fungsi, port, protokol, dan layanan yang tidak penting.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
CM.L2-3.4.7	Membatasi, menonaktifkan, atau mencegah penggunaan program, fungsi, port, protokol, dan layanan yang tidak penting.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.7	Membatasi, menonaktifkan, atau mencegah penggunaan program, fungsi, port, protokol, dan layanan yang tidak penting.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.7	Membatasi, menonaktifkan, atau mencegah penggunaan program, fungsi, port, protokol, dan layanan yang tidak penting.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.7	Membatasi, menonaktifkan, atau mencegah penggunaan program, fungsi, port, protokol, dan layanan yang tidak penting.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.7	Membatasi, menonaktifkan, atau mencegah penggunaan program, fungsi, port, protokol, dan layanan yang tidak penting.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
CM.L2-3.4.7	Membatasi, menonaktifkan, atau mencegah penggunaan program, fungsi, port, protokol, dan layanan yang tidak penting.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.7	Membatasi, menonaktifkan, atau mencegah penggunaan program, fungsi, port, protokol, dan layanan yang tidak penting.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
CM.L2-3.4.7	Membatasi, menonaktifkan, atau mencegah penggunaan program, fungsi, port, protokol, dan layanan yang tidak penting.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.7	Membatasi, menonaktifkan, atau mencegah penggunaan program, fungsi, port, protokol, dan layanan yang tidak penting.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.7	Membatasi, menonaktifkan, atau mencegah penggunaan program, fungsi, port, protokol, dan layanan yang tidak penting.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.7	Membatasi, menonaktifkan, atau mencegah penggunaan program, fungsi, port, protokol, dan layanan yang tidak penting.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.9	Kontrol dan pantau perangkat lunak yang diinstal pengguna.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.9	Kontrol dan pantau perangkat lunak yang diinstal pengguna.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM.L2-3.4.9	Kontrol dan pantau perangkat lunak yang diinstal pengguna.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
IA.L2-3.5.1	Mengidentifikasi pengguna sistem informasi, proses yang bertindak atas nama pengguna, atau perangkat.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.1	Mengidentifikasi pengguna sistem informasi, proses yang bertindak atas nama pengguna, atau perangkat.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
IA.L2-3.5.1	Mengidentifikasi pengguna sistem informasi, proses yang bertindak atas nama pengguna, atau perangkat.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.1	Mengidentifikasi pengguna sistem informasi, proses yang bertindak atas nama pengguna, atau perangkat.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.1	Mengidentifikasi pengguna sistem informasi, proses yang bertindak atas nama pengguna, atau perangkat.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.1	Mengidentifikasi pengguna sistem informasi, proses yang bertindak atas nama pengguna, atau perangkat.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.1	Mengidentifikasi pengguna sistem informasi, proses yang bertindak atas nama pengguna, atau perangkat.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.1	Mengidentifikasi pengguna sistem informasi, proses yang bertindak atas nama pengguna, atau perangkat.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.1	Mengidentifikasi pengguna sistem informasi, proses yang bertindak atas nama pengguna, atau perangkat.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.2	Mengautentikasi (atau memverifi kasi) identitas pengguna, proses, atau perangkat tersebut, sebagai prasyarat untuk memungkinkan akses ke sistem informasi organisasi.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.2	Mengautentikasi (atau memverifikasi) identitas pengguna, proses, atau perangkat tersebut, sebagai prasyarat untuk memungkinkan akses ke sistem informasi organisasi.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.2	Mengautentikasi (atau memverifi kasi) identitas pengguna, proses, atau perangkat tersebut, sebagai prasyarat untuk memungkinkan akses ke sistem informasi organisasi.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastika n otentikasi multi-fak tor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.2	Mengautentikasi (atau memverifi kasi) identitas pengguna, proses, atau perangkat tersebut, sebagai prasyarat untuk memungkinkan akses ke sistem informasi organisasi.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.2	Mengautentikasi (atau memverifikasi) identitas pengguna, proses, atau perangkat tersebut, sebagai prasyarat untuk memungkinkan akses ke sistem informasi organisasi.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.2	Mengautentikasi (atau memverifikasi) identitas pengguna, proses, atau perangkat tersebut, sebagai prasyarat untuk memungkinkan akses ke sistem informasi organisasi.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.3	Gunakan otentikasi multifaktor untuk akses lokal dan jaringan ke akun istimewa dan untuk akses jaringan ke akun yang tidak memiliki hak istimewa.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.3	Gunakan otentikasi multifaktor untuk akses lokal dan jaringan ke akun istimewa dan untuk akses jaringan ke akun yang tidak memiliki hak istimewa.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.3	Gunakan otentikasi multifaktor untuk akses lokal dan jaringan ke akun istimewa dan untuk akses jaringan ke akun yang tidak memiliki hak istimewa.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.3	Gunakan otentikasi multifaktor untuk akses lokal dan jaringan ke akun istimewa dan untuk akses jaringan ke akun yang tidak memiliki hak istimewa.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.6	Nonaktifkan pengidentifikasi setelah periode tidak aktif yang ditentukan.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.6	Nonaktifkan pengidentifikasi setelah periode tidak aktif yang ditentukan.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.7	Menerapkan kompleksitas kata sandi minimum dan perubahan karakter saat kata sandi baru dibuat.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.8	Melarang penggunaan kembali kata sandi untuk sejumlah generasi tertentu.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
IA.L2-3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	alb-http-drop-invalid-header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	alb-http-to-https-pemeriksaan-pengalihan	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
IA.L2-3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
IA.L2-3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
IA.L2-3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
IA.L2-3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
IA.L2-3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
IA.L2-3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	rds-snapshot-encry pted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
IA.L2-3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
IA.L2-3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
IA.L2-3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
IA.L2-3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
IA.L2-3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA.L2-3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR.L2-3.6.1	Menetapkan kemampuan penanganan insiden operasional untuk sistem organisas i yang mencakup persiapan, deteksi, analisis, penahanan , pemulihan, dan aktivitas respons pengguna.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR.L2-3.6.1	Menetapkan kemampuan penanganan insiden operasional untuk sistem organisasi yang mencakup persiapan, deteksi, analisis, penahanan, pemulihan, dan aktivitas respons pengguna.	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan: rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR.L2-3.6.1	Menetapkan kemampuan penanganan insiden operasional untuk sistem organisas i yang mencakup persiapan, deteksi, analisis, penahanan , pemulihan, dan aktivitas respons pengguna.	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR.L2-3.6.1	Menetapkan kemampuan penanganan insiden operasional untuk sistem organisas i yang mencakup persiapan, deteksi, analisis, penahanan , pemulihan, dan aktivitas respons pengguna.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR.L2-3.6.3	Uji kemampuan respons insiden organisasi.	response-plan-tested (Pemeriksaan Proses)	Pastikan respon Insiden dan rencana pemulihan diuji. Ini dapat membantu dalam memahami apakah rencana Anda akan efektif selama insiden dan jika ada celah atau pembaruan yang perlu ditangani.
MA.L2-3.7.5	Memerlukan otentikasi multifaktor untuk membuat sesi pemeliharaan nonlokal dari koneksi jaringan eksternal dan menghentikan koneksi tersebut ketika pemeliharaan nonlokal selesai.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
MA.L2-3.7.5	Memerlukan otentikasi multifaktor untuk membuat sesi pemeliharaan nonlokal dari koneksi jaringan eksternal dan menghentikan koneksi tersebut ketika pemeliharaan nonlokal selesai.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
R.L2-3.11.2	Pindai kerentanan dalam sistem dan aplikasi organisasi secara berkala dan ketika kerentana n baru yang memengaruhi sistem dan aplikasi tersebut diidentifikasi.	ec2- -periksa managedinstance-pa tch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
R.L2-3.11.2	Pindai kerentanan dalam sistem dan aplikasi organisasi secara berkala dan ketika kerentana n baru yang memengaruhi sistem dan aplikasi tersebut diidentifikasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
R.L2-3.11.2	Pindai kerentanan dalam sistem dan aplikasi organisasi secara berkala dan ketika kerentana n baru yang memengaruhi sistem dan aplikasi tersebut diidentifikasi.	guardduty-non-arch ived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasark an tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunak an klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSe v (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratk an oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
R.L2-3.11.2	Pindai kerentanan dalam sistem dan aplikasi organisasi secara berkala dan ketika kerentana n baru yang memengaruhi sistem dan aplikasi tersebut diidentifikasi.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	alb-http-drop-invalid-header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	alb-http-to-https-pemeriksaan-pengalihan	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindunginya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigurasi ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.1	Memantau, mengendalikan, dan melindungi komunikasi organisasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem informasi organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem informasi.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindungi nya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomen dasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaa n enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCES S_KEY_ID dan AWS_SECRE T_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild . Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabk an paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredenal masuk dalam lingkungan proyek Codebuild . AWS Gunakan OAuth alih-alih token akses pribadi atau kredensi masuk untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	rds-cluster-multi-az-diaktifkan	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
SC.L2-3.13.4	Mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.4	Mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
SC.L2-3.13.4	Mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.4	Mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
SC.L2-3.13.4	Mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.4	Mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
SC.L2-3.13.4	Mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.4	Mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
SC.L2-3.13.4	Mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.4	Mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.4	Mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.4	Mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
SC.L2-3.13.4	Mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.4	Mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
SC.L2-3.13.4	Mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.4	Mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.4	Mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.8	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan CUI yang tidak sah selama transmisi kecuali dilindungi oleh perlindungan fisik alternatif.	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
SC.L2-3.13.8	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan CUI yang tidak sah selama transmisi kecuali dilindungi oleh perlindungan fisik alternatif.	alb-http-drop-invalid-header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.8	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan CUI yang tidak sah selama transmisi kecuali dilindungi oleh perlindungan fisik alternatif.	alb-http-to-https-pemeriksaan-pengalihan	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC.L2-3.13.8	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan CUI yang tidak sah selama transmisi kecuali dilindungi oleh perlindungan fisik alternatif.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.8	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan CUI yang tidak sah selama transmisi kecuali dilindungi oleh perlindungan fisik alternatif.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.8	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan CUI yang tidak sah selama transmisi kecuali dilindungi oleh perlindungan fisik alternatif.	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.8	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan CUI yang tidak sah selama transmisi kecuali dilindungi oleh perlindungan fisik alternatif.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
SC.L2-3.13.8	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan CUI yang tidak sah selama transmisi kecuali dilindungi oleh perlindungan fisik alternatif.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.8	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan CUI yang tidak sah selama transmisi kecuali dilindungi oleh perlindungan fisik alternatif.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC.L2-3.13.8	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan CUI yang tidak sah selama transmisi kecuali dilindungi oleh perlindungan fisik alternatif.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.8	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan CUI yang tidak sah selama transmisi kecuali dilindungi oleh perlindungan fisik alternatif.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC.L2-3.13.10	Menetapkan dan mengelola kunci kriptografi untuk kriptografi yang digunakan dalam sistem organisasi.	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.10	Menetapkan dan mengelola kunci kriptografi untuk kriptografi yang digunakan dalam sistem organisasi.	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.15	Lindungi keaslian sesi komunikasi.	alb-http-to-https-pemeriksaan-pengalihan	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC.L2-3.13.15	Lindungi keaslian sesi komunikasi.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.15	Lindungi keaslian sesi komunikasi.	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.15	Lindungi keaslian sesi komunikasi.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
SC.L2-3.13.15	Lindungi keaslian sesi komunikasi.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.15	Lindungi keaslian sesi komunikasi.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC.L2-3.13.16	Lindungi kerahasiaan CUI saat istirahat.	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC.L2-3.13.16	Lindungi kerahasiaan CUI saat istirahat.	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.16	Lindungi kerahasiaan CUI saat istirahat.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrai l jejak Anda.
SC.L2-3.13.16	Lindungi kerahasiaan CUI saat istirahat.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC.L2-3.13.16	Lindungi kerahasiaan CUI saat istirahat.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.16	Lindungi kerahasiaan CUI saat istirahat.	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
SC.L2-3.13.16	Lindungi kerahasiaan CUI saat istirahat.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
SC.L2-3.13.16	Lindungi kerahasiaan CUI saat istirahat.	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.16	Lindungi kerahasiaan CUI saat istirahat.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC.L2-3.13.16	Lindungi kerahasiaan CUI saat istirahat.	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.16	Lindungi kerahasiaan CUI saat istirahat.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
SC.L2-3.13.16	Lindungi kerahasiaan CUI saat istirahat.	s3- default-encryption -kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.16	Lindungi kerahasiaan CUI saat istirahat.	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC.L2-3.13.16	Lindungi kerahasiaan CUI saat istirahat.	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC.L2-3.13.16	Lindungi kerahasiaan CUI saat istirahat.	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC.L2-3.13.16	Lindungi kerahasiaan CUI saat istirahat.	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.1	Mengidentifikasi, melaporkan, dan memperbaiki kelemahan sistem informasi dan informasi secara tepat waktu.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.1	Mengidentifikasi, melaporkan, dan memperbaiki kelemahan sistem informasi dan informasi secara tepat waktu.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.1	Mengidentifikasi, melaporkan, dan memperbaiki kelemahan sistem informasi dan informasi secara tepat waktu.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.2	Memberikan perlindungan dari kode berbahaya di lokasi yang sesuai dalam sistem informasi organisasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.5	Lakukan pemindaian berkala sistem informasi dan pemindaian file secara real-time dari sumber eksternal saat file diunduh, dibuka, atau dieksekusi.	ecr-private-image-scanning-diaktifkan	Pemindaian gambar Amazon Elastic Container Repository (ECR) membantu mengidentifikasi kerentanan perangkat lunak dalam gambar kontainer Anda. Mengaktifkan pemindaian gambar pada repositori ECR menambahkan lapisan verifikasi untuk integritas dan keamanan gambar yang disimpan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.3	Pantau peringatan dan saran keamanan sistem dan ambil tindakan sebagai tanggapan.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.3	Pantau peringatan dan saran keamanan sistem dan ambil tindakan sebagai tanggapan.	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindungi nya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.3	Pantau peringatan dan saran keamanan sistem dan ambil tindakan sebagai tanggapan.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.3	Pantau peringatan dan saran keamanan sistem dan ambil tindakan sebagai tanggapan.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
SI.L2-3.14.3	Pantau peringatan dan saran keamanan sistem dan ambil tindakan sebagai tanggapan.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.3	Pantau peringatan dan saran keamanan sistem dan ambil tindakan sebagai tanggapan.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.3	Pantau peringatan dan saran keamanan sistem dan ambil tindakan sebagai tanggapan.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.3	Pantau peringatan dan saran keamanan sistem dan ambil tindakan sebagai tanggapan.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.3	Pantau peringatan dan saran keamanan sistem dan ambil tindakan sebagai tanggapan.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.6	Memantau sistem organisasi, termasuk lalu lintas komunikasi masuk dan keluar, untuk mendeteksi serangan dan indikator serangan potensial.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.6	Memantau sistem organisasi, termasuk lalu lintas komunikasi masuk dan keluar, untuk mendeteksi serangan dan indikator serangan potensial.	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindunginya dari serangan berbahaya
SI.L2-3.14.6	Memantau sistem organisasi, termasuk lalu lintas komunikasi masuk dan keluar, untuk mendeteksi serangan dan indikator serangan potensial.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.6	Memantau sistem organisasi, termasuk lalu lintas komunikasi masuk dan keluar, untuk mendeteksi serangan dan indikator serangan potensial.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.6	Memantau sistem organisasi, termasuk lalu lintas komunikasi masuk dan keluar, untuk mendeteksi serangan dan indikator serangan potensial.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.6	Memantau sistem organisasi, termasuk lalu lintas komunikasi masuk dan keluar, untuk mendeteksi serangan dan indikator serangan potensial.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.6	Memantau sistem organisasi, termasuk lalu lintas komunikasi masuk dan keluar, untuk mendeteksi serangan dan indikator serangan potensial.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.6	Memantau sistem organisasi, termasuk lalu lintas komunikasi masuk dan keluar, untuk mendeteksi serangan dan indikator serangan potensial.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
SI.L2-3.14.7	Identifikasi penggunaan sistem organisasi yang tidak sah.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.7	Identifikasi penggunaan sistem organisasi yang tidak sah.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
SI.L2-3.14.7	Identifikasi penggunaan sistem organisasi yang tidak sah.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.7	Identifikasi penggunaan sistem organisasi yang tidak sah.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.7	Identifikasi penggunaan sistem organisasi yang tidak sah.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.7	Identifikasi penggunaan sistem organisasi yang tidak sah.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.7	Identifikasi penggunaan sistem organisasi yang tidak sah.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.7	Identifikasi penggunaan sistem organisasi yang tidak sah.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.7	Identifikasi penggunaan sistem organisasi yang tidak sah.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.7	Identifikasi penggunaan sistem organisasi yang tidak sah.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.7	Identifikasi penggunaan sistem organisasi yang tidak sah.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI.L2-3.14.7	Identifikasi penggunaan sistem organisasi yang tidak sah.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk CMMC 2.0 Level 2.

Praktik Terbaik Operasional untuk Layanan Komputasi

Paket kesesuaian ini berisi AWS Config aturan berdasarkan Compute Services. Untuk informasi selengkapnya, lihat Menghitung beban kerja apa pun. Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Layanan Komputasi.

Praktik Terbaik Operasional untuk Ketahanan Data

Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Ketahanan Data.

Praktik Terbaik Operasional untuk Layanan Database

Paket kesesuaian ini berisi AWS Config aturan berdasarkan Layanan Database. Untuk informasi selengkapnya, lihat Database di AWS. Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Layanan Database.

Praktik Terbaik Operasional untuk Data Lakes dan Layanan Analytics

Paket kesesuaian ini berisi AWS Config aturan untuk Data Lakes dan Layanan Analytics. Untuk informasi selengkapnya, lihat Data Lakes and Analytics di AWS. Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Data Lakes dan Layanan Analytics.

Praktik Terbaik Operasional untuk DevOps

Paket kesesuaian ini berisi AWS Config aturan berdasarkan di dalam. DevOps AWS Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Operasional untuk DevOps.

Praktik Terbaik Operasional untuk EC2

Paket kesesuaian ini berisi AWS Config aturan berdasarkan. EC2 Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Operasional untuk EC2.

Praktik Terbaik Operasional untuk Enkripsi dan Manajemen Kunci

Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Enkripsi dan Manajemen Kunci.

Praktik Terbaik Operasional untuk Panduan Keamanan Siber ENISA untuk SMEs

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara panduan Keamanan Siber Badan Uni Eropa untuk Keamanan Siber (ENISA) untuk dan aturan Config yang SMEs dikelola AWS . Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau beberapa panduan Keamanan Siber ENISA untuk kontrol. SMEs Panduan Keamanan Siber ENISA untuk SMEs kontrol dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

Contoh template paket kesesuaian ini berisi pemetaan ke kontrol yang diadaptasi dari panduan Keamanan Siber ENISA untuk. SMEs Panduan Keamanan Siber ENISA SMEs tersedia di panduan Keamanan Siber untuk SMEs - 12 langkah untuk mengamankan bisnis Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_KEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: PUBLIKASIKAN KEBIJAKAN KEAMANAN SIBER	Aturan yang jelas dan spesifik harus diuraikan dalam keamanan siber	security-awareness-program-exists(Pemeriksaan Proses)	Membangun dan memelihara program kesadaran keamanan untuk organisasi Anda. Program kesadaran keamanan mendidik karyawan tentang cara melindungi organisasi mereka dari berbagai pelanggaran atau insiden keamanan.
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	langkah-langkah keamanan yang tepat.		
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	s3- bucket-acl-prohibited	Aturan ini memeriksa untuk melihat apakah Daftar Kontrol Akses (ACLs) digunakan untuk kontrol akses di Bucket Amazon S3. ACLs adalah mekanisme kontrol akses lama untuk bucket Amazon S3 yang AWS mendahului Identity and Access Management (IAM). Sebagai gantinya ACLs, ini adalah praktik terbaik untuk menggunakan kebijakan IAM atau kebijakan bucket S3 untuk mengelola akses ke bucket S3 Anda dengan lebih mudah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	alb-http-drop-invalid-header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain Amazon Elasticsearch Service (Amazon ES) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	efs-access-point-enforce-root-direktori	Menegakkan direktori root untuk jalur akses Amazon Elastic File System (Amazon EFS) membantu membatasi akses data dengan memastikan bahwa pengguna jalur akses hanya dapat menjangkau file dari subdirektori yang ditentukan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	efs-access-point-enforce-identitas pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan penegakan pengguna diaktifkan untuk Amazon Elastic File System (Amazon EFS) Anda. Saat diaktifkan, Amazon EFS mengganti kan pengguna dan grup klien NFS IDs dengan identitas yang dikonfigurasi pada titik akses untuk semua operasi sistem file dan hanya memberikan akses ke identitas pengguna yang diberlakukan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	codebuild-project-artifact-encryption	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk AWS CodeBuild artefak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	codebuild-project-s3-log-terenkripsi	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk AWS CodeBuild log Anda yang disimpan di Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk Amazon Elasticsearch Service diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	kinesis-stream-encrypted	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1_MENGEMBANGKAN BUDAYA KEAMANAN SIBER YANG BAIK: INGAT PERLINDUNGAN DATA	Berdasarkan Peraturan Perlindungan Data Umum Uni Eropa1, setiap SMEs yang memproses atau menyimpan data pribadi milik penduduk Uni Eropa/EEA perlu memastikan bahwa kontrol keamanan yang tepat tersedia untuk melindungi data tersebut. Ini termasuk memastikan bahwa setiap pihak ketiga yang bekerja atas nama UKM memiliki langkah-langkah keamanan yang tepat.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2_BERIKAN PELATIHAN YANG SESUAI	Berikan pelatihan kesadaran keamanan siber secara teratur untuk semua karyawan untuk memastikan mereka dapat mengenali dan menangani berbagai ancaman keamanan siber. Pelatihan ini harus disesuaik an untuk UKM dan fokus pada situasi kehidupan nyata. Memberikan pelatihan keamanan siber khusus bagi mereka yang bertanggu ng jawab untuk mengelola keamanan siber dalam bisnis untuk memastikan mereka akan memiliki keterampilan dan kompetensi yang diperlukan untuk melakukan pekerjaan mereka.	security-awareness -program-exists(Pe meriksaan Proses)	Membangun dan memelihara program kesadaran keamanan untuk organisas i Anda. Program kesadaran keamanan mendidik karyawan tentang cara melindungi organisas i mereka dari berbagai pelanggaran atau insiden keamanan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4_KEMBANGKAN RENCANA RESPONS INSIDEN	Mengembangkan rencana respons insiden formal, yang berisi pedoman, peran, dan tanggung jawab yang jelas yang didokumentasikan untuk memastikan bahwa semua insiden keamanan ditanggapi secara tepat waktu, profesional, dan tepat. Untuk merespons ancaman keamanan dengan cepat, selidiki alat yang dapat memantau dan membuat peringatan ketika aktivitas mencurigakan atau pelanggaran keamanan terjadi.	response-plan-exists-maintained(Pemeriksaan Proses)	Memastikan rencana respons insiden dibuat, dipelihara, dan didistribusikan kepada personel yang bertanggung jawab.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5_SECURE AKSES KE SISTEM	Dorong semua orang untuk menggunakan frasa sandi, kumpulan setidaknya tiga kata umum acak yang digabungkan menjadi frasa yang memberikan kombinasi yang sangat baik antara daya ingat dan keamanan. Jika Anda memilih kata sandi khas: - Buatlah panjang, dengan karakter huruf kecil dan besar, mungkin juga angka dan karakter khusus. - Hindari yang jelas, seperti “kata sandi”, urutan huruf atau angka seperti “abc”, angka seperti “123". - Hindari menggunakan info pribadi yang dapat ditemukan secara online. Dan apakah Anda menggunakan kata sandi atau kata sandi - Jangan menggunakannya kembali di tempat lain. - Jangan membaginya dengan	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	rekan kerja. - Aktifkan Otentikasi Multi-Faktor. - Gunakan pengelola kata sandi khusus.		(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5_SECURE AKSES KE SISTEM	Dorong semua orang untuk menggunakan frasa sandi, kumpulan setidaknya tiga kata umum acak yang digabungkan menjadi frasa yang memberikan kombinasi yang sangat baik antara daya ingat dan keamanan. Jika Anda memilih kata sandi khas: - Buatlah panjang, dengan karakter huruf kecil dan besar, mungkin juga angka dan karakter khusus. - Hindari yang jelas, seperti “kata sandi”, urutan huruf atau angka seperti “abc”, angka seperti “123". - Hindari menggunakan info pribadi yang dapat ditemukan secara online. Dan apakah Anda menggunakan kata sandi atau kata sandi - Jangan menggunakannya kembali di tempat lain. - Jangan membaginya dengan	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	rekan kerja. - Aktifkan Otentikasi Multi-Faktor. - Gunakan pengelola kata sandi khusus.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5_SECURE AKSES KE SISTEM	Dorong semua orang untuk menggunakan frasa sandi, kumpulan setidaknya tiga kata umum acak yang digabungkan menjadi frasa yang memberikan kombinasi yang sangat baik antara daya ingat dan keamanan. Jika Anda memilih kata sandi khas: - Buatlah panjang, dengan karakter huruf kecil dan besar, mungkin juga angka dan karakter khusus. - Hindari yang jelas, seperti “kata sandi”, urutan huruf atau angka seperti “abc”, angka seperti “123". - Hindari menggunakan info pribadi yang dapat ditemukan secara online. Dan apakah Anda menggunakan kata sandi atau kata sandi - Jangan menggunakannya kembali di tempat lain. - Jangan membaginya dengan	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	rekan kerja. - Aktifkan Otentikasi Multi-Faktor. - Gunakan pengelola kata sandi khusus.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5_SECURE AKSES KE SISTEM	Dorong semua orang untuk menggunakan frasa sandi, kumpulan setidaknya tiga kata umum acak yang digabungkan menjadi frasa yang memberikan kombinasi yang sangat baik antara daya ingat dan keamanan. Jika Anda memilih kata sandi khas: - Buatlah panjang, dengan karakter huruf kecil dan besar, mungkin juga angka dan karakter khusus. - Hindari yang jelas, seperti “kata sandi”, urutan huruf atau angka seperti “abc”, angka seperti “123". - Hindari menggunakan info pribadi yang dapat ditemukan secara online. Dan apakah Anda menggunakan kata sandi atau kata sandi - Jangan menggunakannya kembali di tempat lain. - Jangan membaginya dengan	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	rekan kerja. - Aktifkan Otentikasi Multi-Faktor. - Gunakan pengelola kata sandi khusus.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5_SECURE AKSES KE SISTEM	Dorong semua orang untuk menggunakan frasa sandi, kumpulan setidaknya tiga kata umum acak yang digabungkan menjadi frasa yang memberikan kombinasi yang sangat baik antara daya ingat dan keamanan. Jika Anda memilih kata sandi khas: - Buatlah panjang, dengan karakter huruf kecil dan besar, mungkin juga angka dan karakter khusus. - Hindari yang jelas, seperti “kata sandi”, urutan huruf atau angka seperti “abc”, angka seperti “123". - Hindari menggunakan info pribadi yang dapat ditemukan secara online. Dan apakah Anda menggunakan kata sandi atau kata sandi - Jangan menggunakannya kembali di tempat lain. - Jangan membaginya dengan	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	rekan kerja. - Aktifkan Otentikasi Multi-Faktor. - Gunakan pengelola kata sandi khusus.		
PERANGKAT 6_SECURE: JAGA AGAR PERANGKAT LUNAK TETAP DITAMBAL DAN DIPERBARUI	Idealnya menggunakan platform terpusat untuk mengelola patching. Sangat disarankan SMEs untuk: - Secara teratur memperbarui semua perangkat lunak mereka. - Aktifkan pembaruan otomatis bila memungkinkan. - Identifikasi perangkat lunak dan perangkat keras yang memerlukan pembaruan manual. - Mempertimbangkan perangkat seluler dan IoT.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: JAGA AGAR PERANGKAT LUNAK TETAP DITAMBAL DAN DIPERBARUI	Idealnya menggunakan platform terpusat untuk mengelola patching. Sangat disarankan SMEs untuk: - Secara teratur memperbarui semua perangkat lunak mereka. - Aktifkan pembaruan otomatis bila memungkinkan. - Identifikasi perangkat lunak dan perangkat keras yang memerlukan pembaruan manual. - Mempertimbangkan perangkat seluler dan IoT.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: JAGA AGAR PERANGKAT LUNAK TETAP DITAMBAL DAN DIPERBARUI	Idealnya menggunakan platform terpusat untuk mengelola patching. Sangat disarankan SMEs untuk: - Secara teratur memperbarui semua perangkat lunak mereka. - Aktifkan pembaruan otomatis bila memungkinkan. - Identifikasi perangkat lunak dan perangkat keras yang memerlukan pembaruan manual. - Mempertimbangkan perangkat seluler dan IoT.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: JAGA AGAR PERANGKAT LUNAK TETAP DITAMBAL DAN DIPERBARUI	Idealnya menggunakan platform terpusat untuk mengelola patching. Sangat disarankan SMEs untuk: - Secara teratur memperbarui semua perangkat lunak mereka. - Aktifkan pembaruan otomatis bila memungkinkan. - Identifikasi perangkat lunak dan perangkat keras yang memerlukan pembaruan manual. - Mempertimbangkan perangkat seluler dan IoT.	ecs-fargate-latest-platform-versi	Pembaruan dan tambalan keamanan diterapkan secara otomatis untuk tugas Fargate AWS Anda. Jika ditemukan masalah keamanan yang memengaruhi versi platform AWS Fargate, AWS tambal versi platform. Untuk membantu pengelolaan tambalan tugas Amazon Elastic Container Service (ECS) yang menjalankan AWS Fargate, perbarui tugas mandiri layanan Anda untuk menggunakan versi platform terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: JAGA AGAR PERANGKAT LUNAK TETAP DITAMBAL DAN DIPERBARUI	Idealnya menggunakan platform terpusat untuk mengelola patching. Sangat disarankan SMEs untuk: - Secara teratur memperbarui semua perangkat lunak mereka. - Aktifkan pembaruan otomatis bila memungkinkan. - Identifikasi perangkat lunak dan perangkat keras yang memerlukan pembaruan manual. - Mempertimbangkan perangkat seluler dan IoT.	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: JAGA AGAR PERANGKAT LUNAK TETAP DITAMBAL DAN DIPERBARUI	Idealnya menggunakan platform terpusat untuk mengelola patching. Sangat disarankan SMEs untuk: - Secara teratur memperbarui semua perangkat lunak mereka. - Aktifkan pembaruan otomatis bila memungkinkan. - Identifikasi perangkat lunak dan perangkat keras yang memerlukan pembaruan manual. - Mempertimbangkan perangkat seluler dan IoT.	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relational Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: JAGA AGAR PERANGKAT LUNAK TETAP DITAMBAL DAN DIPERBARUI	Idealnya menggunakan platform terpusat untuk mengelola patching. Sangat disarankan SMEs untuk: - Secara teratur memperbarui semua perangkat lunak mereka. - Aktifkan pembaruan otomatis bila memungkinkan. - Identifikasi perangkat lunak dan perangkat keras yang memerlukan pembaruan manual. - Mempertimbangkan perangkat seluler dan IoT.	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, smartphone, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, smartphone, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, smartphone, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, smartphone, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, smartphone, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, smartphone, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	codebuild-project-artifact-encryption	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk AWS CodeBuild artefak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, smartphone, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	codebuild-project-s3-log-terenkripsi	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk AWS CodeBuild log Anda yang disimpan di Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, smartphone, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, smartphone, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, smartphone, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, smartphone, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain Amazon Elasticsearch Service (Amazon ES) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, smartphone, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, smartphone, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, smartphone, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, smartphone, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk Amazon Elasticsearch Service diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, smartphone, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, ponsel cerdas, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, ponsel cerdas, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, ponsel cerdas, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, ponsel cerdas, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	kinesis-stream-encrypted	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, ponsel cerdas, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, ponsel cerdas, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, ponsel cerdas, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, ponsel cerdas, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, ponsel cerdas, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, ponsel cerdas, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	s3- default-encryption -kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, ponsel cerdas, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, ponsel cerdas, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, ponsel cerdas, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, ponsel cerdas, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, ponsel cerdas, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, ponsel cerdas, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PERANGKAT 6_SECURE: ENKRIPSI	Lindungi data dengan mengenkripsinya. SMEsharus memastikan data yang disimpan di perangkat seluler seperti laptop, ponsel cerdas, dan tabel dienkripsi. Untuk data yang ditransfer melalui jaringan publik, seperti WiFi jaringan hotel atau bandara, pastikan bahwa data dienkripsi, baik dengan menggunakan Virtual Private Network (VPN) atau mengakses situs web melalui koneksi aman menggunakan protokol SSL/TLS. Pastikan situs web mereka menggunakan teknologi enkripsi yang sesuai untuk melindungi data klien saat melakukan perjalanan melalui Internet.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7_SECURE JARINGAN ANDA: GUNAKAN FIREWALL	Firewall mengelola lalu lintas yang masuk dan keluar jaringan dan merupakan alat penting dalam melindungi SMEs sistem. Firewall harus digunakan untuk melindungi semua sistem penting, khususnya firewall harus digunakan untuk melindungi jaringan UKM dari Internet.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7_SECURE JARINGAN ANDA: GUNAKAN FIREWALL	Firewall mengelola lalu lintas yang masuk dan keluar jaringan dan merupakan alat penting dalam melindungi SMEs sistem. Firewall harus digunakan untuk melindungi semua sistem penting, khususnya firewall harus digunakan untuk melindungi jaringan UKM dari Internet.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7_SECURE JARINGAN ANDA: GUNAKAN FIREWALL	Firewall mengelola lalu lintas yang masuk dan keluar jaringan dan merupakan alat penting dalam melindungi SMEs sistem. Firewall harus digunakan untuk melindungi semua sistem penting, khususnya firewall harus digunakan untuk melindungi jaringan UKM dari Internet.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7_SECURE JARINGAN ANDA: GUNAKAN FIREWALL	Firewall mengelola lalu lintas yang masuk dan keluar jaringan dan merupakan alat penting dalam melindungi SMEs sistem. Firewall harus digunakan untuk melindungi semua sistem penting, khususnya firewall harus digunakan untuk melindungi jaringan UKM dari Internet.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/ 0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7_SECURE JARINGAN ANDA: GUNAKAN FIREWALL	Firewall mengelola lalu lintas yang masuk dan keluar jaringan dan merupakan alat penting dalam melindungi SMEs sistem. Firewall harus digunakan untuk melindungi semua sistem penting, khususnya firewall harus digunakan untuk melindungi jaringan UKM dari Internet.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7_SECURE JARINGAN ANDA: GUNAKAN FIREWALL	Firewall mengelola lalu lintas yang masuk dan keluar jaringan dan merupakan alat penting dalam melindungi SMEs sistem. Firewall harus digunakan untuk melindungi semua sistem penting, khususnya firewall harus digunakan untuk melindungi jaringan UKM dari Internet.	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindunginya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7_SECURE JARINGAN ANDA: GUNAKAN FIREWALL	Firewall mengelola lalu lintas yang masuk dan keluar jaringan dan merupakan alat penting dalam melindungi SMEs sistem. Firewall harus digunakan untuk melindungi semua sistem penting, khususnya firewall harus digunakan untuk melindungi jaringan UKM dari Internet.	netfw-policy-rule-group-terkait	Kebijakan AWS Network Firewall mendefinisikan bagaimana firewall Anda memantau dan menangani lalu lintas di VPC Amazon. Anda mengonfigurasi grup aturan stateless dan stateful untuk memfilter paket dan arus lalu lintas, dan Anda menentuka n penanganan lalu lintas default.
7_SECURE JARINGAN ANDA: GUNAKAN FIREWALL	Firewall mengelola lalu lintas yang masuk dan keluar jaringan dan merupakan alat penting dalam melindungi SMEs sistem. Firewall harus digunakan untuk melindungi semua sistem penting, khususnya firewall harus digunakan untuk melindungi jaringan UKM dari Internet.	netfw-stateless-rule-group-tidak-kosong	Grup aturan AWS Network Firewall berisi aturan yang menentukan bagaimana firewall Anda memproses lalu lintas di VPC Anda. Grup aturan stateless kosong saat ada dalam kebijakan firewall tidak memproses lalu lintas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7_SECURE JARINGAN ANDA: GUNAKAN FIREWALL	Firewall mengelola lalu lintas yang masuk dan keluar jaringan dan merupakan alat penting dalam melindungi SMEs sistem. Firewall harus digunakan untuk melindungi semua sistem penting, khususnya firewall harus digunakan untuk melindungi jaringan UKM dari Internet.	waf-regional-rule-not-kosong	Pastikan AWS WAF Anda memiliki aturan yang tidak kosong. Aturan tanpa kondisi dapat mengakibatkan perilaku yang tidak diinginkan.
7_SECURE JARINGAN ANDA: GUNAKAN FIREWALL	Firewall mengelola lalu lintas yang masuk dan keluar jaringan dan merupakan alat penting dalam melindungi SMEs sistem. Firewall harus digunakan untuk melindungi semua sistem penting, khususnya firewall harus digunakan untuk melindungi jaringan UKM dari Internet.	waf-regional-rulegroup-not-kosong	Pastikan AWS WAF Anda memiliki grup aturan yang tidak kosong. Grup aturan yang kosong dapat mengakibatkan perilaku yang tidak diinginkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7_SECURE JARINGAN ANDA: GUNAKAN FIREWALL	Firewall mengelola lalu lintas yang masuk dan keluar jaringan dan merupakan alat penting dalam melindungi SMEs sistem. Firewall harus digunakan untuk melindungi semua sistem penting, khususnya firewall harus digunakan untuk melindungi jaringan UKM dari Internet.	waf-regional-webacl-not-kosong	Web ACL yang dilampirkan ke AWS WAF dapat berisi kumpulan aturan dan kelompok aturan untuk memeriksa dan mengontrol permintaan web. Jika ACL Web kosong, lalu lintas web lewat tanpa terdeteksi atau ditindaklanjuti oleh WAF.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7_SECURE JARINGAN ANDA: TINJAU SOLUSI AKSES JARAK JAUH	SMEs harus secara teratur meninjau alat akses jarak jauh apa pun untuk memastikannya aman, terutama: - Pastikan semua perangkat lunak akses jarak jauh ditambal dan diperbarui. - Batasi akses jarak jauh dari lokasi geografis yang mencurigakan atau alamat IP tertentu. - Batasi akses jarak jauh staf hanya ke sistem dan komputer yang mereka butuhkan untuk pekerjaan mereka. - Menerapkan kata sandi yang kuat untuk akses jarak jauh dan jika memungkinkan memungkinkan otentikasi multi-faktor. - Pastikan pemantauan dan peringatan diaktifkan untuk memperingatkan dugaan serangan atau aktivitas	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mencurigakan yang tidak biasa.		(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7_SECURE JARINGAN ANDA: TINJAU SOLUSI AKSES JARAK JAUH	SMEs harus secara teratur meninjau alat akses jarak jauh apa pun untuk memastikannya aman, terutama: - Pastikan semua perangkat lunak akses jarak jauh ditambal dan diperbarui. - Batasi akses jarak jauh dari lokasi geografis yang mencurigakan atau alamat IP tertentu. - Batasi akses jarak jauh staf hanya ke sistem dan komputer yang mereka butuhkan untuk pekerjaan mereka. - Menerapkan kata sandi yang kuat untuk akses jarak jauh dan jika memungkinkan memungkinkan otentikasi multi-faktor. - Pastikan pemantauan dan peringatan diaktifkan untuk memperingatkan dugaan serangan atau aktivitas	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mencurigakan yang tidak biasa.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7_SECURE JARINGAN ANDA: TINJAU SOLUSI AKSES JARAK JAUH	SMEs harus secara teratur meninjau alat akses jarak jauh apa pun untuk memastikannya aman, terutama: - Pastikan semua perangkat lunak akses jarak jauh ditambal dan diperbarui. - Batasi akses jarak jauh dari lokasi geografis yang mencurigakan atau alamat IP tertentu. - Batasi akses jarak jauh staf hanya ke sistem dan komputer yang mereka butuhkan untuk pekerjaan mereka. - Menerapkan kata sandi yang kuat untuk akses jarak jauh dan jika memungkinkan memungkinkan otentikasi multi-faktor. - Pastikan pemantauan dan peringatan diaktifkan untuk memperingatkan dugaan serangan atau aktivitas	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mencurigakan yang tidak biasa.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7_SECURE JARINGAN ANDA: TINJAU SOLUSI AKSES JARAK JAUH	SMEs harus secara teratur meninjau alat akses jarak jauh apa pun untuk memastikannya aman, terutama: - Pastikan semua perangkat lunak akses jarak jauh ditambal dan diperbarui. - Batasi akses jarak jauh dari lokasi geografis yang mencurigakan atau alamat IP tertentu. - Batasi akses jarak jauh staf hanya ke sistem dan komputer yang mereka butuhkan untuk pekerjaan mereka. - Menerapkan kata sandi yang kuat untuk akses jarak jauh dan jika memungkinkan memungkinkan otentikasi multi-faktor. - Pastikan pemantauan dan peringatan diaktifkan untuk memperingatkan dugaan serangan atau aktivitas	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mencurigakan yang tidak biasa.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7_SECURE JARINGAN ANDA: TINJAU SOLUSI AKSES JARAK JAUH	SMEs harus secara teratur meninjau alat akses jarak jauh apa pun untuk memastikannya aman, terutama: - Pastikan semua perangkat lunak akses jarak jauh ditambal dan diperbarui. - Batasi akses jarak jauh dari lokasi geografis yang mencurigakan atau alamat IP tertentu. - Batasi akses jarak jauh staf hanya ke sistem dan komputer yang mereka butuhkan untuk pekerjaan mereka. - Menerapkan kata sandi yang kuat untuk akses jarak jauh dan jika memungkinkan memungkinkan otentikasi multi-faktor. - Pastikan pemantauan dan peringatan diaktifkan untuk memperingatkan dugaan serangan atau aktivitas	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mencurigakan yang tidak biasa.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7_SECURE JARINGAN ANDA: TINJAU SOLUSI AKSES JARAK JAUH	SMEs harus secara teratur meninjau alat akses jarak jauh apa pun untuk memastikannya aman, terutama: - Pastikan semua perangkat lunak akses jarak jauh ditambal dan diperbarui. - Batasi akses jarak jauh dari lokasi geografis yang mencurigakan atau alamat IP tertentu. - Batasi akses jarak jauh staf hanya ke sistem dan komputer yang mereka butuhkan untuk pekerjaan mereka. - Menerapkan kata sandi yang kuat untuk akses jarak jauh dan jika memungkinkan memungkinkan otentikasi multi-faktor. - Pastikan pemantauan dan peringatan diaktifkan untuk memperingatkan dugaan serangan atau aktivitas	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mencurigakan yang tidak biasa.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7_SECURE JARINGAN ANDA: TINJAU SOLUSI AKSES JARAK JAUH	SMEs harus secara teratur meninjau alat akses jarak jauh apa pun untuk memastikannya aman, terutama: - Pastikan semua perangkat lunak akses jarak jauh ditambal dan diperbarui. - Batasi akses jarak jauh dari lokasi geografis yang mencurigakan atau alamat IP tertentu. - Batasi akses jarak jauh staf hanya ke sistem dan komputer yang mereka butuhkan untuk pekerjaan mereka. - Menerapkan kata sandi yang kuat untuk akses jarak jauh dan jika memungkinkan memungkinkan otentikasi multi-faktor. - Pastikan pemantauan dan peringatan diaktifkan untuk memperingatkan dugaan serangan atau aktivitas	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mencurigakan yang tidak biasa.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7_SECURE JARINGAN ANDA: TINJAU SOLUSI AKSES JARAK JAUH	SMEs harus secara teratur meninjau alat akses jarak jauh apa pun untuk memastikannya aman, terutama: - Pastikan semua perangkat lunak akses jarak jauh ditambal dan diperbarui. - Batasi akses jarak jauh dari lokasi geografis yang mencurigakan atau alamat IP tertentu. - Batasi akses jarak jauh staf hanya ke sistem dan komputer yang mereka butuhkan untuk pekerjaan mereka. - Menerapkan kata sandi yang kuat untuk akses jarak jauh dan jika memungkinkan memungkinkan otentikasi multi-faktor. - Pastikan pemantauan dan peringatan diaktifkan untuk memperingatkan dugaan serangan atau aktivitas	elasticsearch-logs-to-cloudwatch	Pastikan domain layanan Amazon Elasticsearch mengaktifkan log kesalahan dan dialirkan ke Log CloudWatch Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mencurigakan yang tidak biasa.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7_SECURE JARINGAN ANDA: TINJAU SOLUSI AKSES JARAK JAUH	SMEs harus secara teratur meninjau alat akses jarak jauh apa pun untuk memastika nnya aman, terutama: - Pastikan semua perangkat lunak akses jarak jauh ditambal dan diperbarui. - Batasi akses jarak jauh dari lokasi geografis yang mencuriga kan atau alamat IP tertentu. - Batasi akses jarak jauh staf hanya ke sistem dan komputer yang mereka butuhkan untuk pekerjaan mereka. - Menerapka n kata sandi yang kuat untuk akses jarak jauh dan jika memungkinkan memungkinkan otentikasi multi-faktor. - Pastikan pemantaua n dan peringata n diaktifkan untuk memperingatkan dugaan serangan atau aktivitas	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mencurigakan yang tidak biasa.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7_SECURE JARINGAN ANDA: TINJAU SOLUSI AKSES JARAK JAUH	SMEs harus secara teratur meninjau alat akses jarak jauh apa pun untuk memastikannya aman, terutama: - Pastikan semua perangkat lunak akses jarak jauh ditambal dan diperbarui. - Batasi akses jarak jauh dari lokasi geografis yang mencurigakan atau alamat IP tertentu. - Batasi akses jarak jauh staf hanya ke sistem dan komputer yang mereka butuhkan untuk pekerjaan mereka. - Menerapkan kata sandi yang kuat untuk akses jarak jauh dan jika memungkinkan memungkinkan otentikasi multi-faktor. - Pastikan pemantauan dan peringatan diaktifkan untuk memperingatkan dugaan serangan atau aktivitas	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mencurigakan yang tidak biasa.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7_SECURE JARINGAN ANDA: TINJAU SOLUSI AKSES JARAK JAUH	SMEs harus secara teratur meninjau alat akses jarak jauh apa pun untuk memastikannya aman, terutama: - Pastikan semua perangkat lunak akses jarak jauh ditambal dan diperbarui. - Batasi akses jarak jauh dari lokasi geografis yang mencurigakan atau alamat IP tertentu. - Batasi akses jarak jauh staf hanya ke sistem dan komputer yang mereka butuhkan untuk pekerjaan mereka. - Menerapkan kata sandi yang kuat untuk akses jarak jauh dan jika memungkinkan memungkinkan otentikasi multi-faktor. - Pastikan pemantauan dan peringatan diaktifkan untuk memperingatkan dugaan serangan atau aktivitas	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mencurigakan yang tidak biasa.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7_SECURE JARINGAN ANDA: TINJAU SOLUSI AKSES JARAK JAUH	SMEs harus secara teratur meninjau alat akses jarak jauh apa pun untuk memastikannya aman, terutama: - Pastikan semua perangkat lunak akses jarak jauh ditambal dan diperbarui. - Batasi akses jarak jauh dari lokasi geografis yang mencurigakan atau alamat IP tertentu. - Batasi akses jarak jauh staf hanya ke sistem dan komputer yang mereka butuhkan untuk pekerjaan mereka. - Menerapkan kata sandi yang kuat untuk akses jarak jauh dan jika memungkinkan memungkinkan otentikasi multi-faktor. - Pastikan pemantauan dan peringatan diaktifkan untuk memperingatkan dugaan serangan atau aktivitas	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mencurigakan yang tidak biasa.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7_SECURE JARINGAN ANDA: TINJAU SOLUSI AKSES JARAK JAUH	SMEs harus secara teratur meninjau alat akses jarak jauh apa pun untuk memastikannya aman, terutama: - Pastikan semua perangkat lunak akses jarak jauh ditambal dan diperbarui. - Batasi akses jarak jauh dari lokasi geografis yang mencurigakan atau alamat IP tertentu. - Batasi akses jarak jauh staf hanya ke sistem dan komputer yang mereka butuhkan untuk pekerjaan mereka. - Menerapkan kata sandi yang kuat untuk akses jarak jauh dan jika memungkinkan memungkinkan otentikasi multi-faktor. - Pastikan pemantauan dan peringatan diaktifkan untuk memperingatkan dugaan serangan atau aktivitas	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mencurigakan yang tidak biasa.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7_SECURE JARINGAN ANDA: TINJAU SOLUSI AKSES JARAK JAUH	SMEs harus secara teratur meninjau alat akses jarak jauh apa pun untuk memastika nnya aman, terutama: - Pastikan semua perangkat lunak akses jarak jauh ditambal dan diperbarui. - Batasi akses jarak jauh dari lokasi geografis yang mencuriga kan atau alamat IP tertentu. - Batasi akses jarak jauh staf hanya ke sistem dan komputer yang mereka butuhkan untuk pekerjaan mereka. - Menerapka n kata sandi yang kuat untuk akses jarak jauh dan jika memungkinkan memungkinkan otentikasi multi-faktor. - Pastikan pemantaua n dan peringata n diaktifkan untuk memperingatkan dugaan serangan atau aktivitas	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mencurigakan yang tidak biasa.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7_SECURE JARINGAN ANDA: TINJAU SOLUSI AKSES JARAK JAUH	SMEs harus secara teratur meninjau alat akses jarak jauh apa pun untuk memastikannya aman, terutama: - Pastikan semua perangkat lunak akses jarak jauh ditambal dan diperbarui. - Batasi akses jarak jauh dari lokasi geografis yang mencurigakan atau alamat IP tertentu. - Batasi akses jarak jauh staf hanya ke sistem dan komputer yang mereka butuhkan untuk pekerjaan mereka. - Menerapkan kata sandi yang kuat untuk akses jarak jauh dan jika memungkinkan memungkinkan otentikasi multi-faktor. - Pastikan pemantauan dan peringatan diaktifkan untuk memperingatkan dugaan serangan atau aktivitas	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mencurigakan yang tidak biasa.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7_SECURE JARINGAN ANDA: TINJAU SOLUSI AKSES JARAK JAUH	SMEs harus secara teratur meninjau alat akses jarak jauh apa pun untuk memastikannya aman, terutama: - Pastikan semua perangkat lunak akses jarak jauh ditambal dan diperbarui. - Batasi akses jarak jauh dari lokasi geografis yang mencurigakan atau alamat IP tertentu. - Batasi akses jarak jauh staf hanya ke sistem dan komputer yang mereka butuhkan untuk pekerjaan mereka. - Menerapkan kata sandi yang kuat untuk akses jarak jauh dan jika memungkinkan memungkinkan otentikasi multi-faktor. - Pastikan pemantauan dan peringatan diaktifkan untuk memperingatkan dugaan serangan atau aktivitas	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mencurigakan yang tidak biasa.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7_SECURE JARINGAN ANDA: TINJAU SOLUSI AKSES JARAK JAUH	SMEs harus secara teratur meninjau alat akses jarak jauh apa pun untuk memastikannya aman, terutama: - Pastikan semua perangkat lunak akses jarak jauh ditambal dan diperbarui. - Batasi akses jarak jauh dari lokasi geografis yang mencurigakan atau alamat IP tertentu. - Batasi akses jarak jauh staf hanya ke sistem dan komputer yang mereka butuhkan untuk pekerjaan mereka. - Menerapkan kata sandi yang kuat untuk akses jarak jauh dan jika memungkinkan memungkinkan otentikasi multi-faktor. - Pastikan pemantauan dan peringatan diaktifkan untuk memperingatkan dugaan serangan atau aktivitas	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mencurigakan yang tidak biasa.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7_SECURE JARINGAN ANDA: TINJAU SOLUSI AKSES JARAK JAUH	SMEs harus secara teratur meninjau alat akses jarak jauh apa pun untuk memastikannya aman, terutama: - Pastikan semua perangkat lunak akses jarak jauh ditambal dan diperbarui. - Batasi akses jarak jauh dari lokasi geografis yang mencurigakan atau alamat IP tertentu. - Batasi akses jarak jauh staf hanya ke sistem dan komputer yang mereka butuhkan untuk pekerjaan mereka. - Menerapkan kata sandi yang kuat untuk akses jarak jauh dan jika memungkinkan memungkinkan otentikasi multi-faktor. - Pastikan pemantauan dan peringatan diaktifkan untuk memperingatkan dugaan serangan atau aktivitas	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mencurigakan yang tidak biasa.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7_SECURE JARINGAN ANDA: TINJAU SOLUSI AKSES JARAK JAUH	SMEs harus secara teratur meninjau alat akses jarak jauh apa pun untuk memastikannya aman, terutama: - Pastikan semua perangkat lunak akses jarak jauh ditambal dan diperbarui. - Batasi akses jarak jauh dari lokasi geografis yang mencurigakan atau alamat IP tertentu. - Batasi akses jarak jauh staf hanya ke sistem dan komputer yang mereka butuhkan untuk pekerjaan mereka. - Menerapkan kata sandi yang kuat untuk akses jarak jauh dan jika memungkinkan memungkinkan otentikasi multi-faktor. - Pastikan pemantauan dan peringatan diaktifkan untuk memperingatkan dugaan serangan atau aktivitas	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositori data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mencurigakan yang tidak biasa.		
PENCADANGAN 9_AMAN	Untuk memungkinkan pemulihan formasi kunci, cadangan harus dipertahankan karena merupakan cara yang efektif untuk pulih dari bencana seperti serangan ransomware. Aturan pencadangan berikut harus berlaku: - cadangan teratur dan otomatis bila memungkinkan, - cadangan diadakan secara terpisah dari lingkungan produksi UKM, - cadangan dienkripsi, terutama jika mereka akan dipindahkan antar lokasi, - kemampuan untuk secara teratur memulihkan data dari cadangan diuji. Idealnya, tes reguler pemulihan penuh dari awal hingga akhir harus dilakukan.	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PENCADANGAN 9_AMAN	Untuk memungkinkan pemulihan formasi kunci, cadangan harus dipertahankan karena merupakan cara yang efektif untuk pulih dari bencana seperti serangan ransomware. Aturan pencadangan berikut harus berlaku: - cadangan teratur dan otomatis bila memungkinkan, - cadangan diadakan secara terpisah dari lingkungan produksi UKM, - cadangan dienkripsi, terutama jika mereka akan dipindahkan antar lokasi, - kemampuan untuk secara teratur memulihkan data dari cadangan diuji. Idealnya, tes reguler pemulihan penuh dari awal hingga akhir harus dilakukan.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PENCADANGAN 9_AMAN	Untuk memungkinkan pemulihan formasi kunci, cadangan harus dipertahankan karena merupakan cara yang efektif untuk pulih dari bencana seperti serangan ransomwar e. Aturan pencadang an berikut harus berlaku: - cadangan teratur dan otomatis bila memungkinkan, - cadangan diadakan secara terpisah dari lingkungan produksi UKM, - cadangan dienkripsi, terutama jika mereka akan dipindahkan antar lokasi, - kemampuan untuk secara teratur memulihkan data dari cadangan diuji. Idealnya, tes reguler pemulihan penuh dari awal hingga akhir harus dilakukan.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PENCADANGAN 9_AMAN	Untuk memungkinkan pemulihan formasi kunci, cadangan harus dipertahankan karena merupakan cara yang efektif untuk pulih dari bencana seperti serangan ransomware. Aturan pencadangan berikut harus berlaku: - cadangan teratur dan otomatis bila memungkinkan, - cadangan diadakan secara terpisah dari lingkungan produksi UKM, - cadangan dienkripsi, terutama jika mereka akan dipindahkan antar lokasi, - kemampuan untuk secara teratur memulihkan data dari cadangan diuji. Idealnya, tes reguler pemulihan penuh dari awal hingga akhir harus dilakukan.	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PENCADANGAN 9_AMAN	Untuk memungkinkan pemulihan formasi kunci, cadangan harus dipertahankan karena merupakan cara yang efektif untuk pulih dari bencana seperti serangan ransomwar e. Aturan pencadang an berikut harus berlaku: - cadangan teratur dan otomatis bila memungkinkan, - cadangan diadakan secara terpisah dari lingkungan produksi UKM, - cadangan dienkripsi, terutama jika mereka akan dipindahkan antar lokasi, - kemampuan untuk secara teratur memulihkan data dari cadangan diuji. Idealnya, tes reguler pemulihan penuh dari awal hingga akhir harus dilakukan.	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadang an data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkin kan Anda untuk mengatur parameter requiredRetentionD ays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisas i Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PENCADANGAN 9_AMAN	Untuk memungkinkan pemulihan formasi kunci, cadangan harus dipertahankan karena merupakan cara yang efektif untuk pulih dari bencana seperti serangan ransomwar e. Aturan pencadang an berikut harus berlaku: - cadangan teratur dan otomatis bila memungkinkan, - cadangan diadakan secara terpisah dari lingkungan produksi UKM, - cadangan dienkripsi, terutama jika mereka akan dipindahkan antar lokasi, - kemampuan untuk secara teratur memulihkan data dari cadangan diuji. Idealnya, tes reguler pemulihan penuh dari awal hingga akhir harus dilakukan.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PENCADANGAN 9_AMAN	Untuk memungkinkan pemulihan formasi kunci, cadangan harus dipertahankan karena merupakan cara yang efektif untuk pulih dari bencana seperti serangan ransomwar e. Aturan pencadang an berikut harus berlaku: - cadangan teratur dan otomatis bila memungkinkan, - cadangan diadakan secara terpisah dari lingkungan produksi UKM, - cadangan dienkripsi, terutama jika mereka akan dipindahkan antar lokasi, - kemampuan untuk secara teratur memulihkan data dari cadangan diuji. Idealnya, tes reguler pemulihan penuh dari awal hingga akhir harus dilakukan.	dynamodb-in-backup-plan	Untuk membantu proses pencadang an data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PENCADANGAN 9_AMAN	Untuk memungkinkan pemulihan formasi kunci, cadangan harus dipertahankan karena merupakan cara yang efektif untuk pulih dari bencana seperti serangan ransomware. Aturan pencadangan berikut harus berlaku: - cadangan teratur dan otomatis bila memungkinkan, - cadangan diadakan secara terpisah dari lingkungan produksi UKM, - cadangan dienkripsi, terutama jika mereka akan dipindahkan antar lokasi, - kemampuan untuk secara teratur memulihkan data dari cadangan diuji. Idealnya, tes reguler pemulihan penuh dari awal hingga akhir harus dilakukan.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan cadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PENCADANGAN 9_AMAN	Untuk memungkinkan pemulihan formasi kunci, cadangan harus dipertahankan karena merupakan cara yang efektif untuk pulih dari bencana seperti serangan ransomwar e. Aturan pencadang an berikut harus berlaku: - cadangan teratur dan otomatis bila memungkinkan, - cadangan diadakan secara terpisah dari lingkungan produksi UKM, - cadangan dienkripsi, terutama jika mereka akan dipindahkan antar lokasi, - kemampuan untuk secara teratur memulihkan data dari cadangan diuji. Idealnya, tes reguler pemulihan penuh dari awal hingga akhir harus dilakukan.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PENCADANGAN 9_AMAN	Untuk memungkinkan pemulihan formasi kunci, cadangan harus dipertahankan karena merupakan cara yang efektif untuk pulih dari bencana seperti serangan ransomwar e. Aturan pencadang an berikut harus berlaku: - cadangan teratur dan otomatis bila memungkinkan, - cadangan diadakan secara terpisah dari lingkungan produksi UKM, - cadangan dienkripsi, terutama jika mereka akan dipindahkan antar lokasi, - kemampuan untuk secara teratur memulihkan data dari cadangan diuji. Idealnya, tes reguler pemulihan penuh dari awal hingga akhir harus dilakukan.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PENCADANGAN 9_AMAN	Untuk memungkinkan pemulihan formasi kunci, cadangan harus dipertahankan karena merupakan cara yang efektif untuk pulih dari bencana seperti serangan ransomwar e. Aturan pencadang an berikut harus berlaku: - cadangan teratur dan otomatis bila memungkinkan, - cadangan diadakan secara terpisah dari lingkungan produksi UKM, - cadangan dienkripsi, terutama jika mereka akan dipindahkan antar lokasi, - kemampuan untuk secara teratur memulihkan data dari cadangan diuji. Idealnya, tes reguler pemulihan penuh dari awal hingga akhir harus dilakukan.	efs-in-backup-plan	Untuk membantu proses pencadang an data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PENCADANGAN 9_AMAN	Untuk memungkinkan pemulihan formasi kunci, cadangan harus dipertahankan karena merupakan cara yang efektif untuk pulih dari bencana seperti serangan ransomwar e. Aturan pencadang an berikut harus berlaku: - cadangan teratur dan otomatis bila memungkinkan, - cadangan diadakan secara terpisah dari lingkungan produksi UKM, - cadangan dienkripsi, terutama jika mereka akan dipindahkan antar lokasi, - kemampuan untuk secara teratur memulihkan data dari cadangan diuji. Idealnya, tes reguler pemulihan penuh dari awal hingga akhir harus dilakukan.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PENCADANGAN 9_AMAN	Untuk memungkinkan pemulihan formasi kunci, cadangan harus dipertahankan karena merupakan cara yang efektif untuk pulih dari bencana seperti serangan ransomwar e. Aturan pencadang an berikut harus berlaku: - cadangan teratur dan otomatis bila memungkinkan, - cadangan diadakan secara terpisah dari lingkungan produksi UKM, - cadangan dienkripsi, terutama jika mereka akan dipindahkan antar lokasi, - kemampuan untuk secara teratur memulihkan data dari cadangan diuji. Idealnya, tes reguler pemulihan penuh dari awal hingga akhir harus dilakukan.	fsx-resources-prot ected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PENCADANGAN 9_AMAN	Untuk memungkinkan pemulihan formasi kunci, cadangan harus dipertahankan karena merupakan cara yang efektif untuk pulih dari bencana seperti serangan ransomwar e. Aturan pencadang an berikut harus berlaku: - cadangan teratur dan otomatis bila memungkinkan, - cadangan diadakan secara terpisah dari lingkungan produksi UKM, - cadangan dienkripsi, terutama jika mereka akan dipindahkan antar lokasi, - kemampuan untuk secara teratur memulihkan data dari cadangan diuji. Idealnya, tes reguler pemulihan penuh dari awal hingga akhir harus dilakukan.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PENCADANGAN 9_AMAN	Untuk memungkinkan pemulihan formasi kunci, cadangan harus dipertahankan karena merupakan cara yang efektif untuk pulih dari bencana seperti serangan ransomwar e. Aturan pencadang an berikut harus berlaku: - cadangan teratur dan otomatis bila memungkinkan, - cadangan diadakan secara terpisah dari lingkungan produksi UKM, - cadangan dienkripsi, terutama jika mereka akan dipindahkan antar lokasi, - kemampuan untuk secara teratur memulihkan data dari cadangan diuji. Idealnya, tes reguler pemulihan penuh dari awal hingga akhir harus dilakukan.	rds-resources-prot ected-by-rencana cadangan	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon Relationa l Database Service (Amazon RDS) Anda merupakan AWS bagian dari paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PENCADANGAN 9_AMAN	Untuk memungkinkan pemulihan formasi kunci, cadangan harus dipertahankan karena merupakan cara yang efektif untuk pulih dari bencana seperti serangan ransomwar e. Aturan pencadang an berikut harus berlaku: - cadangan teratur dan otomatis bila memungkinkan, - cadangan diadakan secara terpisah dari lingkungan produksi UKM, - cadangan dienkripsi, terutama jika mereka akan dipindahkan antar lokasi, - kemampuan untuk secara teratur memulihkan data dari cadangan diuji. Idealnya, tes reguler pemulihan penuh dari awal hingga akhir harus dilakukan.	redshift-backup-en abled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifka n untuk cluster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PENCADANGAN 9_AMAN	Untuk memungkinkan pemulihan formasi kunci, cadangan harus dipertahankan karena merupakan cara yang efektif untuk pulih dari bencana seperti serangan ransomwar e. Aturan pencadang an berikut harus berlaku: - cadangan teratur dan otomatis bila memungkinkan, - cadangan diadakan secara terpisah dari lingkungan produksi UKM, - cadangan dienkripsi, terutama jika mereka akan dipindahkan antar lokasi, - kemampuan untuk secara teratur memulihkan data dari cadangan diuji. Idealnya, tes reguler pemulihan penuh dari awal hingga akhir harus dilakukan.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11_AMAN SITUS ONLINE	Penting SMEs untuk memastikan bahwa situs web online mereka dikonfigurasi dan dipelihara dengan cara yang aman dan bahwa data pribadi atau detail keuangan apa pun, seperti data kartu kredit, dilindung i dengan tepat. Ini akan memerluka n menjalankan tes keamanan reguler terhadap situs web untuk mengident ifikasi kelemahan keamanan potensial dan melakukan tinjauan rutin untuk memastikan situs dipertahankan dan diperbarui dengan benar.	vuln-management-pl an-exists(Pemeriks aan Proses)	Pastikan rencana manajemen kerentana n dikembangkan dan diimplementasikan untuk memiliki proses yang ditentukan secara formal untuk mengatasi kerentanan di lingkungan Anda.

Templat

Template tersedia di GitHub: Panduan Praktik Terbaik Operasional untuk Keamanan Siber ENISA untuk. SMEs

Praktik Terbaik Operasional untuk Esquema Nacional de Seguridad (ENS) Rendah

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara Spanyol Esquema Nacional de Seguridad (ENS) Kontrol kerangka kerja rendah dan aturan Config terkelola. AWS Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau beberapa kontrol ENS Low Spanyol. Kontrol ENS Spanyol dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

Templat paket kesesuaian sampel ini berisi pemetaan ke kontrol dalam kerangka kerja ENS Low Spanyol, seperti yang terakhir diperbarui pada 2020/10/23.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
Anex II 4.1.2.a); b); c)	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic

ID Kontrol	AWS Aturan Config	Bimbingan
		Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	elb-cross-zone-load-menyeim bangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkat kan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
Anex II 4.1.2.a); b); c)	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	sns-encrypted-kms	Untuk membantu melindung i data saat istirahat, pastikan topik Amazon Simple Notificat ion Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	alb-http-to-https-pengalihan-periksa	Untuk membantu melindung i data dalam perjalanan, pastikan Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	api-gw-cache-enabled-dan-di enkripsi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifika t SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
Anex II 4.1.2.a); b); c)	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
Anex II 4.1.2.a); b); c)	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
Anex II 4.1.2.a); b); c)	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.
Anex II 4.1.2.a); b); c)	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
Anex II 4.1.2.a); b); c)	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindung i data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
Anex II 4.1.2.a); b); c)	elb-deletion-protection-ena bled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifka n. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
Anex II 4.1.2.a); b); c)	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
Anex II 4.1.2.a); b); c)	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independe n yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	rds-cluster-multi-az-diaktifkan	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independe n yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	rds-storage-encrypted	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastika n bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberika n informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	redshift-cluster-kms-enabled	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerluka n enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	s3- bucket-ssl-requests-only	Untuk membantu melindung i data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerluka n permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	sagemaker-endpoint-configur ation-kms-kunci-dikonfigurasi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	secretsmanager-using-cmk	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimpleme ntasikan untuk mencapai persyaratan ketahanan . Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-S ite VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.b)	ec2- security-group-attached-to -eni-periodik	Aturan ini memastikan grup keamanan dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) atau ke ENI. Aturan ini membantu memantau kelompok keamanan yang tidak digunakan dalam inventaris dan pengelolaan lingkungan Anda.
Anex II 4.1.2.b)	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapka n status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigura si aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.b)	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan , sesuai dengan standar organisasi Anda.
Anex II 4.1.2.b)	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirk an ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.b)	terlampir eip	Aturan ini memastikan Elastic IPs dialokasikan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan . Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.
Anex II 4.1.2.b)	vpc-network-acl-unused-periksa	Aturan ini memastikan bahwa daftar kontrol akses jaringan Amazon Virtual Private Cloud (VPC) sedang digunakan . Pemantauan untuk daftar kontrol akses jaringan yang tidak digunakan dapat membantu inventaris dan pengelolaan lingkungan Anda yang akurat.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.1.a)	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.
Anex II 4.2.1.a); b)	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.4	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.
Anex II 4.2.4	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkin kan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
Anex II 4.2.4	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.5	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.5.bajo.a)	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.5.bajo.c)	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
Anex II 4.2.6.bajo.c)	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.6.bajo.c)	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimk an file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.6.bajo.c)	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
Anex II 4.2.6.bajo.c)	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
Anex II 4.2.6.bajo.c)	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.6.bajo.c)	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
Anex II 4.2.6.bajo.c)	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
Anex II 4.2.6.bajo.c)	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.6.bajo.c)	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.
Anex II 4.2.6.bajo.c)	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.6.bajo.c)	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.
Anex II 4.2.6.bajo.c)	vpc-flow-logs-enabled	Log aliran VPC menyediak an catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.7.BAJO	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
Anex II 4.2.7.BAJO	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahk an lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.7.BAJO	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
Anex II 4.2.7.BAJO	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.1	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapka n status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigura si aplikasi, dan detail lainnya tentang lingkungan Anda.
Anex II 4.3.1	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan , sesuai dengan standar organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.1	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirk an ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.
Anex II 4.3.1	terlampir eip	Aturan ini memastikan Elastic IPs dialokasikan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan . Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.1	vpc-network-acl-unused-periksa	Aturan ini memastikan bahwa daftar kontrol akses jaringan Amazon Virtual Private Cloud (VPC) sedang digunakan . Pemantauan untuk daftar kontrol akses jaringan yang tidak digunakan dapat membantu inventaris dan pengelolaan lingkungan Anda yang akurat.
Anex II 4.3.2.b)	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.2.b)	api-gw-associated-with-waf	AWS WAF memungkin kan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindung inya dari serangan berbahaya
Anex II 4.3.2.b)	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.2.b)	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
Anex II 4.3.2.b)	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspo s informasi tentang akun, sumber daya, dan proses internal Anda.
Anex II 4.3.2.b)	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.2.b)	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
Anex II 4.3.2.b)	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
Anex II 4.3.2.b)	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.2.b)	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
Anex II 4.3.2.b)	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkin kan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabk an akses tidak sah ke sumber daya VPC Amazon.
Anex II 4.3.2.b)	lambda-function-public-acce ss-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.2.b)	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyarat an untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.2.b)	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearc h Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
Anex II 4.3.2.b)	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.2.b)	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
Anex II 4.3.2.b)	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.2.b)	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,338 9,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.2.b)	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
Anex II 4.3.2.b)	s3- -dilarang bucket-level-publi c-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.2.b)	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
Anex II 4.3.2.b)	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
Anex II 4.3.2.b)	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.2.b)	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
Anex II 4.3.2.b)	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.2.b)	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.
Anex II 4.3.4.c)	vuln-management-plan-exists (Pemeriksaan Proses)	Pastikan rencana manajemen kerentanan dikembangkan dan diimplementasikan untuk memiliki proses yang ditentukan secara formal untuk mengatasi kerentanan di lingkungan Anda. Ini dapat mencakup alat manajemen kerentanan, irama pemindaian lingkungan, peran dan tanggung jawab.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.8.BAJO	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
Anex II 4.3.8.BAJO	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.8.BAJO	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
Anex II 4.3.8.BAJO	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
Anex II 4.3.8.BAJO	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.8.BAJO	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
Anex II 4.3.8.BAJO	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
Anex II 4.3.8.BAJO	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.8.BAJO	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.
Anex II 4.3.8.BAJO	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.8.BAJO	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.
Anex II 4.3.8.BAJO	vpc-flow-logs-enabled	Log aliran VPC menyediak an catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.10.b)	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
Anex II 4.3.10.b)	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.10.d)	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersedi aan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.
Anex II 4.6.1	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.6.2.DASAR	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
Anex II 5.2.3	security-awareness-program-exists (Pemeriksaan Proses)	Membangun dan memelihar a program kesadaran keamanan untuk organisas i Anda. Program kesadaran keamanan mendidik karyawan tentang cara melindung i organisasi mereka dari berbagai pelanggaran atau insiden keamanan.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.4.3.bajo.a)	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
Anex II 5.6.1.c)	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild. Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.
Anex II 5.6.1.c)	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber Bitbucket GitHub atau Bitbucket tidak berisi token akses pribadi, kredensyal masuk dalam lingkungan proyek Codebuild. AWS Gunakan OAuth alih-alih token akses pribadi atau kredensyal masuk untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
Anex II 5.7.3	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 5.7.3	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 5.7.3	rds-snapshot-encrypted	Pastikan enkripsi diaktifka n untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 5.7.3	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 5.7.3	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	alb-http-to-https-pengalihan-periksa	Untuk membantu melindung i data dalam perjalanan, pastikan Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 5.7.3	api-gw-cache-enabled-dan-di enkripsi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 5.7.3	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifika t SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
Anex II 5.7.3	cloudwatch-log-group-encrypted	Untuk membantu melindung i data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
Anex II 5.7.3	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
Anex II 5.7.3	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindung i data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
Anex II 5.7.3	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
Anex II 5.7.3	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 5.7.3	rds-storage-encrypted	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
Anex II 5.7.3	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerluka n enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 5.7.3	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
Anex II 5.7.3	s3- bucket-ssl-requests-only	Untuk membantu melindung i data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerluka n permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 5.7.3	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 5.7.4	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.4	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.
Anex II 5.8.2	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.8.2	api-gw-associated-with-waf	AWS WAF memungkin kan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindung inya dari serangan berbahaya
Seni 14.4	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 16	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.
Seni. 16	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkin kan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
Seni. 16	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 20.2	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relationa l Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.
Seni 20.2	ec2- -periksa managedin stance-patch-compliance-sta tus	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 20.2	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.
Seni 20.2	vuln-management-plan-exists (Pemeriksaan Proses)	Pastikan rencana manajemen kerentanan dikembangkan dan diimplementasikan untuk memiliki proses yang ditentukan secara formal untuk mengatasi kerentanan di lingkungan Anda. Ini dapat mencakup alat manajemen kerentanan, irama pemindaian lingkungan, peran dan tanggung jawab.
Seni. 21.1	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	ec2- ebs-encryption-by-default	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Seni. 21.1	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.
Seni. 21.1	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
Seni. 21.1	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Seni. 21.1	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Seni. 21.1	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Seni. 21.1	sns-encrypted-kms	Untuk membantu melindung i data saat istirahat, pastikan topik Amazon Simple Notificat ion Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	alb-http-to-https-pengalihan-periksa	Untuk membantu melindung i data dalam perjalanan, pastikan Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Seni. 21.1	api-gw-cache-enabled-dan-di enkripsi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Seni. 21.1	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifika t SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
Seni. 21.1	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.
Seni. 21.1	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.
Seni. 21.1	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
Seni. 21.1	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindung i data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
Seni. 21.1	elb-deletion-protection-ena bled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifka n. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
Seni. 21.1	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
Seni. 21.1	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independe n yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	rds-cluster-multi-az-diaktifkan	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independe n yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	rds-storage-encrypted	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Seni. 21.1	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastika n bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberika n informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	redshift-cluster-kms-enabled	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Seni. 21.1	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerluka n enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Seni. 21.1	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	s3- bucket-ssl-requests-only	Untuk membantu melindung i data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerluka n permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Seni. 21.1	sagemaker-endpoint-configur ation-kms-kunci-dikonfigurasi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	secretsmanager-using-cmk	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Seni. 21.1	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimpleme ntasikan untuk mencapai persyaratan ketahanan . Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-S ite VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
Seni 22	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspo s informasi tentang akun, sumber daya, dan proses internal Anda.
Seni 22	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
Seni 22	ebs-snapshot-public-restora ble-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihka n secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
Seni 22	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearc h Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
Seni 22	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkin kan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabk an akses tidak sah ke sumber daya VPC Amazon.
Seni 22	lambda-function-public-acce ss-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyarat an untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearc h Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
Seni 22	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
Seni 22	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,338 9,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
Seni 22	s3- -dilarang bucket-level-publi c-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
Seni 22	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
Seni 22	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
Seni 22	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.
Seni 23	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 23	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimk an file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 23	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
Seni 23	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
Seni 23	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 23	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
Seni 23	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
Seni 23	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 23	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.
Seni 23	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 23	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.
Seni 23	vpc-flow-logs-enabled	Log aliran VPC menyediak an catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 25	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
Seni. 25	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 25	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
Seni. 25	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relational Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 25	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.
Seni. 25	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 25	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan cadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.
Seni. 25	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediak an tambahan, kapasitas khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 25	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.
Seni. 25	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 25	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihka n setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Esquema Nacional de Seguridad (ENS) Rendah.

Praktik Terbaik Operasional untuk Medium Esquema Nacional de Seguridad (ENS)

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara kontrol kerangka kerja Medium Esquema Nacional de Seguridad (ENS) Spanyol dan aturan Config terkelola. AWS Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau beberapa kontrol ENS Medium Spanyol. Kontrol ENS Spanyol dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

Templat paket kesesuaian sampel ini berisi pemetaan ke kontrol dalam kerangka ENS Medium Spanyol, seperti yang terakhir diperbarui pada 2020/10/23.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.1.2.a); b); c)	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
Anezo II 4.1.2.a); b); c)	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anezo II 4.1.2.a); b); c)	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi

ID Kontrol	AWS Aturan Config	Bimbingan
		memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anezo II 4.1.2.a); b); c)	elb-cross-zone-load-menyeim bangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkat kan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.
Anezo II 4.1.2.a); b); c)	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.1.2.a); b); c)	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
Anezo II 4.1.2.a); b); c)	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anezo II 4.1.2.a); b); c)	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.1.2.a); b); c)	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anezo II 4.1.2.a); b); c)	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	sns-encrypted-kms	Untuk membantu melindung i data saat istirahat, pastikan topik Amazon Simple Notificat ion Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	alb-http-to-https-pengalihan-periksa	Untuk membantu melindung i data dalam perjalanan, pastikan bahwa Applicati on Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	api-gw-cache-enabled-dan-di enkripsi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifika t SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
Anex II 4.1.2.a); b); c)	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus, atau memalsukan CloudTrail file log tanpa deteksi.
Anex II 4.1.2.a); b); c)	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.
Anex II 4.1.2.a); b); c)	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
Anex II 4.1.2.a); b); c)	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindung i data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
Anex II 4.1.2.a); b); c)	elb-deletion-protection-ena bled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifka n. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
Anex II 4.1.2.a); b); c)	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
Anex II 4.1.2.a); b); c)	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independe n yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	rds-cluster-multi-az-diaktifkan	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independe n yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	rds-storage-encrypted	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastika n bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberika n informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	redshift-cluster-kms-enabled	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerluka n enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	s3- bucket-ssl-requests-only	Untuk membantu melindung i data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerluka n permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	sagemaker-endpoint-configur ation-kms-kunci-dikonfigurasi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	secretsmanager-using-cmk	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimpleme ntasikan untuk mencapai persyaratan ketahanan . Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-S ite VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.b)	ec2- security-group-attached-to -eni-periodik	Aturan ini memastikan grup keamanan dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) atau ke ENI. Aturan ini membantu memantau kelompok keamanan yang tidak digunakan dalam inventaris dan pengelolaan lingkungan Anda.
Anex II 4.1.2.b)	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapka n status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigura si aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.b)	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan , sesuai dengan standar organisasi Anda.
Anex II 4.1.2.b)	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirk an ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.b)	terlampir eip	Aturan ini memastikan Elastic IPs dialokasikan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan . Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.
Anex II 4.1.2.b)	vpc-network-acl-unused-periksa	Aturan ini memastikan bahwa daftar kontrol akses jaringan Amazon Virtual Private Cloud (VPC) sedang digunakan . Pemantauan untuk daftar kontrol akses jaringan yang tidak digunakan dapat membantu inventaris dan pengelolaan lingkungan Anda yang akurat.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.1.a)	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.
Anex II 4.2.1.a); 4.2.1.b)	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.4	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.
Anex II 4.2.4	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkin kan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabun gkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
Anex II 4.2.4	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_ bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.5	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.5.a)	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.5.c)	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
Anezo II 4.2.6.bajo.c)	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
Anex II 4.2.6.c)	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.6.c)	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimk an file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.6.c)	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
Anex II 4.2.6.c)	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
Anex II 4.2.6.c)	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.6.c)	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
Anezo II 4.2.6.c)	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
Anezo II 4.2.6.c)	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.2.6.c)	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifka n. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.
Anezo II 4.2.6.c)	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.2.6.c)	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
Anex II 4.2.7	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.7	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahk an lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
Anex II 4.2.7	root-account-hardware-mfa-d iaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.7	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifka n untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
Anex II 4.3.1	ec2- security-group-attached-to -eni-periodik	Aturan ini memastikan grup keamanan dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) atau ke ENI. Aturan ini membantu memantau kelompok keamanan yang tidak digunakan dalam inventaris dan pengelolaan lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.1	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapka n status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigura si aplikasi, dan detail lainnya tentang lingkungan Anda.
Anex II 4.3.1	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan , sesuai dengan standar organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.1	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirk an ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.
Anex II 4.3.1	terlampir eip	Aturan ini memastikan Elastic IPs dialokasikan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan . Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.1	vpc-network-acl-unused-periksa	Aturan ini memastikan bahwa daftar kontrol akses jaringan Amazon Virtual Private Cloud (VPC) sedang digunakan . Pemantauan untuk daftar kontrol akses jaringan yang tidak digunakan dapat membantu inventaris dan pengelolaan lingkungan Anda yang akurat.
Anezo II 4.3.2.b)	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.3.2.b)	api-gw-associated-with-waf	AWS WAF memungkin kan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindung inya dari serangan berbahaya
Anezo II 4.3.2.b)	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
Anezo II 4.3.2.b)	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspo s informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.3.2.b)	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
Anezo II 4.3.2.b)	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
Anezo II 4.3.2.b)	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.3.2.b)	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearc h Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
Anezo II 4.3.2.b)	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.3.2.b)	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.
Anezo II 4.3.2.b)	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.3.2.b)	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.
Anezo II 4.3.2.b)	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigurasi ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.3.2.b)	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearc h Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
Anezo II 4.3.2.b)	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.3.2.b)	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
Anezo II 4.3.2.b)	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.3.2.b)	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,338 9,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.3.2.b)	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
Anezo II 4.3.2.b)	s3- -dilarang bucket-level-publi c-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.3.2.b)	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
Anezo II 4.3.2.b)	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
Anezo II 4.3.2.b)	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.3.2.b)	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
Anezo II 4.3.2.b)	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.3.2.b)	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam grup keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.
Anezo II 4.3.4.c)	vuln-management-plan-exists (Pemeriksaan Proses)	Pastikan rencana manajemen kerentanan dikembangkan dan diimplementasikan untuk memiliki proses yang ditentukan secara formal untuk mengatasi kerentanan di lingkungan Anda. Ini dapat mencakup alat manajemen kerentanan, irama pemindaian lingkungan, peran dan tanggung jawab.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.6	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
Anezo II 4.3.7.a)	response-plan-exists-mainta ined (Pemeriksaan Proses)	Memastikan rencana respons insiden dibuat, dipelihara, dan didistribusikan kepada personel yang bertanggu ng jawab. Memiliki rencana respons yang diperbarui dan didokumentasikan secara formal dapat membantu memastikan personel respons memahami peran, tanggung jawab, dan proses yang harus diikuti selama insiden.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.8	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
Anex II 4.3.8	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.8	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
Anex II 4.3.8	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
Anex II 4.3.8	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.8	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
Anex II 4.3.8	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
Anex II 4.3.8	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.8	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifka n. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.
Anex II 4.3.8	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.8	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
Anezo II 4.3.8.BAJO	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
Anezo II 4.3.8.MEDIO	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.3.10.b)	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
Anezo II 4.3.10.b)	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus, atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.3.10.d)	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersedi aan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.
Anex II 4.6.1	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.6.2	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
Anex II 4.6.2	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.2.3	security-awareness-program-exists (Pemeriksaan Proses)	Membangun dan memelihara program kesadaran keamanan untuk organisasi Anda. Program kesadaran keamanan mendidik karyawan tentang cara melindungi organisasi mereka dari berbagai pelanggaran atau insiden keamanan.
Anex II 5.4.2	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 5.4.2	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.4.2	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 5.4.2	alb-http-to-https-pengalihan-periksa	Untuk membantu melindung i data dalam perjalanan, pastikan bahwa Applicati on Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 5.4.2	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifika t SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.4.2	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindung i data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
Anex II 5.4.2	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerluka n enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 5.4.2	s3- bucket-ssl-requests-only	Untuk membantu melindung i data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerluka n permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 5.4.2.MEDIO	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
Anex II 5.4.3	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.4.3	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan membantu melindung i data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
Anex II 5.4.3	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 5.4.3	alb-http-to-https-pengalihan-periksa	Untuk membantu melindung i data dalam perjalanan, pastikan bahwa Applicati on Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.4.3	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifika t SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
Anex II 5.4.3	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindung i data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
Anex II 5.4.3	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerluka n enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.4.3	s3- bucket-ssl-requests-only	Untuk membantu melindung i data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerluka n permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anezo II 5.4.3.MEDIO	opensearch-logs-to-cloudwat ch	Pastikan domain OpenSearc h Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpan an dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 5.4.3.a)	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
Anezo II 5.6.1.c)	codebuild-project-envvar-awscred-periksa	Pastikan kredensyal otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild. Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.
Anezo II 5.6.1.c)	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredensyal masuk dalam lingkungan proyek Codebuild. AWS Gunakan OAuth alih-alih token akses pribadi atau kredensyal masuk untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
Anex II 5.7.3	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 5.7.3	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 5.7.3	rds-snapshot-encrypted	Pastikan enkripsi diaktifka n untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 5.7.3	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 5.7.3	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	alb-http-to-https-pengalihan-periksa	Untuk membantu melindung i data dalam perjalanan, pastikan bahwa Applicati on Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 5.7.3	api-gw-cache-enabled-dan-di enkripsi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 5.7.3	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifika t SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
Anex II 5.7.3	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
Anex II 5.7.3	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
Anex II 5.7.3	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindung i data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
Anex II 5.7.3	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
Anex II 5.7.3	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 5.7.3	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
Anex II 5.7.3	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 5.7.3	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
Anex II 5.7.3	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 5.7.3	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 5.7.4	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.4	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.
Anex II 5.8.2	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.8.2	api-gw-associated-with-waf	AWS WAF memungkin kan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindung inya dari serangan berbahaya
Anezo II 5.8.3.b)	alb-waf-enabled	Pastikan AWS WAF diaktifka n pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 5.8.3.b)	api-gw-associated-with-waf	AWS WAF memungkin kan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindung inya dari serangan berbahaya
Anezo II 5.8.3.b)	elb-cross-zone-load-menyeim bangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkat kan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 5.8.3.b)	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
Anezo II 5.8.3.b)	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 5.8.3.b)	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 5.8.3.b)	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independe n yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 5.8.3.b)	rds-cluster-multi-az-diaktifkan	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independe n yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 5.8.3.b)	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimpleme ntasikan untuk mencapai persyaratan ketahanan . Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-S ite VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.
Seni 14.4	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 16	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.
Seni. 16	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkin kan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
Seni. 16	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 20.2	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relationa l Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.
Seni 20.2	ec2- -periksa managedin stance-patch-compliance-sta tus	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 20.2	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.
Seni 20.2	vuln-management-plan-exists (Pemeriksaan Proses)	Pastikan rencana manajemen kerentanan dikembangkan dan diimplementasikan untuk memiliki proses yang ditentukan secara formal untuk mengatasi kerentanan di lingkungan Anda. Ini dapat mencakup alat manajemen kerentanan, irama pemindaian lingkungan, peran dan tanggung jawab.
Seni. 21.1	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	ec2- ebs-encryption-by-default	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Seni. 21.1	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.
Seni. 21.1	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
Seni. 21.1	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Seni. 21.1	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Seni. 21.1	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Seni. 21.1	sns-encrypted-kms	Untuk membantu melindung i data saat istirahat, pastikan topik Amazon Simple Notificat ion Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	alb-http-to-https-pengalihan-periksa	Untuk membantu melindung i data dalam perjalanan, pastikan bahwa Applicati on Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Seni. 21.1	api-gw-cache-enabled-dan-di enkripsi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Seni. 21.1	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifika t SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
Seni. 21.1	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus, atau memalsukan CloudTrail file log tanpa deteksi.
Seni. 21.1	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.
Seni. 21.1	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
Seni. 21.1	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindung i data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
Seni. 21.1	elb-deletion-protection-ena bled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifka n. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
Seni. 21.1	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
Seni. 21.1	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independe n yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	rds-cluster-multi-az-diaktifkan	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independe n yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	rds-storage-encrypted	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Seni. 21.1	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastika n bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberika n informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	redshift-cluster-kms-enabled	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Seni. 21.1	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerluka n enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Seni. 21.1	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	s3- bucket-ssl-requests-only	Untuk membantu melindung i data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerluka n permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Seni. 21.1	sagemaker-endpoint-configur ation-kms-kunci-dikonfigurasi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	secretsmanager-using-cmk	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Seni. 21.1	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimpleme ntasikan untuk mencapai persyaratan ketahanan . Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-S ite VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
Seni 22	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
Seni 22	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
Seni 22	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
Seni 22	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
Seni 22	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkin kan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabk an akses tidak sah ke sumber daya VPC Amazon.
Seni 22	lambda-function-public-acce ss-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyarat an untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearc h Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
Seni 22	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
Seni 22	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,338 9,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
Seni 22	s3- -dilarang bucket-level-publi c-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
Seni 22	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
Seni 22	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
Seni 22	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam grup keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.
Seni 23	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 23	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimk an file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 23	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
Seni 23	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
Seni 23	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 23	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
Seni 23	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
Seni 23	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 23	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.
Seni 23	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 23	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.
Seni 23	vpc-flow-logs-enabled	Log aliran VPC menyediak an catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 24.1	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
Seni. 24.2	response-plan-exists-mainta ined (Pemeriksaan Proses)	Memastikan rencana respons insiden dibuat, dipelihara, dan didistribusikan kepada personel yang bertanggu ng jawab. Memiliki rencana respons yang diperbarui dan didokumentasikan secara formal dapat membantu memastikan personel respons memahami peran, tanggung jawab, dan proses yang harus diikuti selama insiden.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 25	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
Seni. 25	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 25	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
Seni. 25	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relational Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 25	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.
Seni. 25	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 25	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadang an berkelanjutan dari tabel Anda selama 35 hari terakhir.
Seni. 25	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediak an tambahan, kapasitas khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 25	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.
Seni. 25	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 25	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihka n setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Medium Esquema Nacional de Seguridad (ENS).

Praktik Terbaik Operasional untuk Esquema Nacional de Seguridad (ENS) High

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara Spanyol Esquema Nacional de Seguridad (ENS) Kontrol kerangka kerja tinggi dan aturan Config terkelola. AWS Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau beberapa kontrol ENS High Spanyol. Kontrol ENS Spanyol dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

Templat paket kesesuaian sampel ini berisi pemetaan ke kontrol dalam kerangka kerja ENS High Spanyol, seperti yang terakhir diperbarui pada 2021/07/09.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.1.ALTO	annual-risk-assessment-performed (Pemeriksaan proses)	Lakukan penilaian risiko tahunan pada organisasi Anda. Penilaian risiko dapat membantu dalam menentukan kemungkinan dan dampak dari risiko dan/atau kerentanan yang diidentifikasi yang mempengaruhi suatu organisasi.
4.2.1.b)	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.
4.2.5.alto.a)	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna

ID Kontrol	AWS Aturan Config	Bimbingan
		root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.
Anex II 4.1.2.a); b); c)	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
Anex II 4.1.2.a); b); c)	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
Anex II 4.1.2.a); b); c)	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	sns-encrypted-kms	Untuk membantu melindung i data saat istirahat, pastikan topik Amazon Simple Notificat ion Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	alb-http-to-https-pengalihan-periksa	Untuk membantu melindung i data dalam perjalanan, pastikan bahwa Applicati on Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	api-gw-cache-enabled-dan-di enkripsi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifika t SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
Anex II 4.1.2.a); b); c)	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
Anex II 4.1.2.a); b); c)	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
Anex II 4.1.2.a); b); c)	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.
Anex II 4.1.2.a); b); c)	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
Anex II 4.1.2.a); b); c)	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
Anex II 4.1.2.a); b); c)	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
Anex II 4.1.2.a); b); c)	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
Anex II 4.1.2.a); b); c)	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) menyediakan ketersediaan dan daya tahan yang ditingkatkan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	rds-cluster-multi-az-diaktifkan	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) menyediakan ketersediaan dan daya tahan yang ditingkatkan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	rds-storage-encrypted	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastika n bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberika n informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	redshift-cluster-kms-enabled	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerluka n enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	s3- bucket-ssl-requests-only	Untuk membantu melindung i data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerluka n permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	sagemaker-endpoint-configur ation-kms-kunci-dikonfigurasi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.a); b); c)	secretsmanager-using-cmk	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 4.1.2.a); b); c)	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimpleme ntasikan untuk mencapai persyaratan ketahanan . Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-S ite VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.b)	ec2- security-group-attached-to -eni-periodik	Aturan ini memastikan grup keamanan dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) atau ke ENI. Aturan ini membantu memantau kelompok keamanan yang tidak digunakan dalam inventaris dan pengelolaan lingkungan Anda.
Anex II 4.1.2.b)	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapka n status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigura si aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.b)	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan , sesuai dengan standar organisasi Anda.
Anex II 4.1.2.b)	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirk an ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.1.2.b)	terlampir eip	Aturan ini memastikan Elastic yang IPs dialokasi kan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan . Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.
Anex II 4.1.2.b)	vpc-network-acl-unused-periksa	Aturan ini memastikan bahwa daftar kontrol akses jaringan Amazon Virtual Private Cloud (VPC) sedang digunakan . Pemantauan untuk daftar kontrol akses jaringan yang tidak digunakan dapat membantu inventaris dan pengelolaan lingkungan Anda yang akurat.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.1.a)	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.
Anex II 4.2.4	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.4	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
Anex II 4.2.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.4	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_ bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs
Anex II 4.2.5	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.2.5.bajo.a)	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.2.5.bajo.c)	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
Anezo II 4.2.6.alto.b)	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
Anezo II 4.2.6.alto.b)	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.2.6.alto.b)	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
Anezo II 4.2.6.alto.b)	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.2.6.bajo.c)	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
Anezo II 4.2.6.bajo.c)	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.2.6.bajo.c)	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
Anezo II 4.2.6.bajo.c)	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
Anezo II 4.2.6.bajo.c)	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.2.6.bajo.c)	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
Anezo II 4.2.6.bajo.c)	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
Anezo II 4.2.6.bajo.c)	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.2.6.bajo.c)	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.
Anezo II 4.2.6.bajo.c)	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.2.6.bajo.c)	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.
Anezo II 4.2.6.bajo.c)	vpc-flow-logs-enabled	Log aliran VPC menyediak an catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.7.BAJO	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
Anex II 4.2.7.BAJO	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahk an lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.2.7.BAJO	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
Anex II 4.2.7.BAJO	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.1	ec2- security-group-attached-to -eni-periodik	Aturan ini memastikan grup keamanan dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) atau ke ENI. Aturan ini membantu memantau kelompok keamanan yang tidak digunakan dalam inventaris dan pengelolaan lingkungan Anda.
Anex II 4.3.1	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapka n status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigura si aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.1	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan , sesuai dengan standar organisasi Anda.
Anex II 4.3.1	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirk an ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.1	terlampir eip	Aturan ini memastikan Elastic IPs dialokasikan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan . Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.
Anex II 4.3.1	vpc-network-acl-unused-periksa	Aturan ini memastikan bahwa daftar kontrol akses jaringan Amazon Virtual Private Cloud (VPC) sedang digunakan . Pemantauan untuk daftar kontrol akses jaringan yang tidak digunakan dapat membantu inventaris dan pengelolaan lingkungan Anda yang akurat.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.2.b)	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.
Anex II 4.3.2.b)	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindungiinya dari serangan berbahaya

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.2.b)	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.
Anex II 4.3.2.b)	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.2.b)	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
Anex II 4.3.2.b)	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspo s informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.2.b)	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
Anex II 4.3.2.b)	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
Anex II 4.3.2.b)	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.2.b)	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearc h Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
Anex II 4.3.2.b)	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.2.b)	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkin kan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabk an akses tidak sah ke sumber daya VPC Amazon.
Anex II 4.3.2.b)	lambda-function-public-acce ss-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.2.b)	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyarat an untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.2.b)	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearc h Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
Anex II 4.3.2.b)	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.2.b)	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
Anex II 4.3.2.b)	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.2.b)	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,338 9,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
Anex II 4.3.2.b)	s3- -dilarang bucket-level-publi c-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.2.b)	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
Anex II 4.3.2.b)	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
Anex II 4.3.2.b)	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.2.b)	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
Anex II 4.3.2.b)	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.2.b)	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.
Anex II 4.3.4.c)	vuln-management-plan-exists (Pemeriksaan Proses)	Pastikan rencana manajemen kerentanan dikembangkan dan diimplementasikan untuk memiliki proses yang ditentukan secara formal untuk mengatasi kerentanan di lingkungan Anda. Ini dapat mencakup alat manajemen kerentanan, irama pemindaian lingkungan, peran dan tanggung jawab.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.6	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
Anex II 4.3.7.media.a)	response-plan-exists-mainta ined (Pemeriksaan Proses)	Memastikan rencana respons insiden dibuat, dipelihara, dan didistribusikan kepada personel yang bertanggu ng jawab. Memiliki rencana respons yang diperbarui dan didokumentasikan secara formal dapat membantu memastikan personel respons memahami peran, tanggung jawab, dan proses yang harus diikuti selama insiden.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.3.8.BAJO	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
Anezo II 4.3.8.BAJO	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.3.8.BAJO	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
Anezo II 4.3.8.BAJO	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
Anezo II 4.3.8.BAJO	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.3.8.BAJO	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
Anezo II 4.3.8.BAJO	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
Anezo II 4.3.8.BAJO	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.3.8.BAJO	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.
Anezo II 4.3.8.BAJO	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.3.8.BAJO	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.
Anezo II 4.3.8.BAJO	vpc-flow-logs-enabled	Log aliran VPC menyediak an catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.3.8.MEDIO	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
Anezo II 4.3.8.MEDIO	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.3.8.MEDIO	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
Anezo II 4.3.8.MEDIO	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
Anezo II 4.3.8.MEDIO	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.3.8.MEDIO	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
Anezo II 4.3.8.MEDIO	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
Anezo II 4.3.8.MEDIO	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.3.8.MEDIO	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.
Anezo II 4.3.8.MEDIO	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.3.8.MEDIO	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.
Anezo II 4.3.8.MEDIO	vpc-flow-logs-enabled	Log aliran VPC menyediak an catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.10.b)	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
Anex II 4.3.10.b)	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 4.3.10.d)	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersedi aan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.
Anex II 4.6.1	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 4.6.2.ALTO	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan: rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Aneexo II 4.6.2.DASAR	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
Anezo II 4.6.2.MEDIA	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.2.3	security-awareness-program-exists (Pemeriksaan Proses)	Membangun dan memelihar a program kesadaran keamanan untuk organisas i Anda. Program kesadaran keamanan mendidik karyawan tentang cara melindung i organisasi mereka dari berbagai pelanggaran atau insiden keamanan.
Anex II 5.2.4	security-awareness-program-exists (Pemeriksaan Proses)	Membangun dan memelihar a program kesadaran keamanan untuk organisas i Anda. Program kesadaran keamanan mendidik karyawan tentang cara melindung i organisasi mereka dari berbagai pelanggaran atau insiden keamanan.
Anex II 5.2.5	security-awareness-program-exists (Pemeriksaan Proses)	Membangun dan memelihar a program kesadaran keamanan untuk organisas i Anda. Program kesadaran keamanan mendidik karyawan tentang cara melindung i organisasi mereka dari berbagai pelanggaran atau insiden keamanan.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 5.4.2.MEDIO	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anezo II 5.4.2.MEDIO	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
Anezo II 5.4.2.MEDIO	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 5.4.2.MEDIO	alb-http-to-https-pengalihan-periksa	Untuk membantu melindung i data dalam perjalanan, pastikan bahwa Applicati on Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anezo II 5.4.2.MEDIO	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifika t SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
Anezo II 5.4.2.MEDIO	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certifica te Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 5.4.2.MEDIO	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
Anezo II 5.4.2.MEDIO	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anezo II 5.4.2.MEDIO	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.4.3.bajo.a)	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
Anezo II 5.4.3.MEDIO	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anezo II 5.4.3.MEDIO	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certifica te Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 5.4.3.MEDIO	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anezo II 5.4.3.MEDIO	alb-http-to-https-pengalihan-periksa	Untuk membantu melindung i data dalam perjalanan, pastikan bahwa Applicati on Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anezo II 5.4.3.MEDIO	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifika t SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 5.4.3.MEDIO	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
Anezo II 5.4.3.MEDIO	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
Anezo II 5.4.3.MEDIO	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anezo II 5.4.3.MEDIO	s3- bucket-ssl-requests-only	Untuk membantu melindung i data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerluka n permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 5.6.1.c)	codebuild-project-envvar-aw scred-periksa	Pastikan kredensyal otentikas i AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_ KEY tidak ada dalam lingkungan proyek AWS Codebuild. Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabk an paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.6.1.c)	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredenal masuk dalam lingkungan proyek Codebuild. AWS Gunakan OAuth alih-alih token akses pribadi atau kredensyal masuk untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.
Anex II 5.7.3	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
Anex II 5.7.3	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 5.7.3	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 5.7.3	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 5.7.3	sagemaker-notebook-instance -kms-kunci-dikonfigurasi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 5.7.3	sns-encrypted-kms	Untuk membantu melindung i data saat istirahat, pastikan topik Amazon Simple Notificat ion Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	alb-http-to-https-pengalihan-periksa	Untuk membantu melindung i data dalam perjalanan, pastikan bahwa Applicati on Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 5.7.3	api-gw-cache-enabled-dan-di enkripsi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 5.7.3	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifika t SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
Anex II 5.7.3	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
Anex II 5.7.3	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
Anex II 5.7.3	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certifica te Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
Anex II 5.7.3	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
Anex II 5.7.3	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 5.7.3	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
Anex II 5.7.3	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Anex II 5.7.3	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
Anex II 5.7.3	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.3	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 5.7.3	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Anex II 5.7.4	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.7.4	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.
Anex II 5.8.2	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.8.2	api-gw-associated-with-waf	AWS WAF memungkin kan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindung inya dari serangan berbahaya
Anex II 5.8.3.medio.b)	alb-waf-enabled	Pastikan AWS WAF diaktifka n pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.8.3.medio.b)	api-gw-associated-with-waf	AWS WAF memungkin kan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindung inya dari serangan berbahaya
Anex II 5.8.3.medio.b)	elb-cross-zone-load-menyeim bangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkat kan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.8.3.medio.b)	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
Anex II 5.8.3.medio.b)	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.8.3.medio.b)	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.8.3.medio.b)	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) menyediakan ketersediaan dan daya tahan yang ditingkatkan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.8.3.medio.b)	rds-cluster-multi-az-diaktifkan	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) menyediakan ketersediaan dan daya tahan yang ditingkatkan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
Anex II 5.8.3.medio.b)	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimpleme ntasikan untuk mencapai persyaratan ketahanan . Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-S ite VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.
Seni 14.4	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 16	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.
Seni. 16	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkin kan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
Seni. 16	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 20.2	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relationa l Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.
Seni 20.2	ec2- -periksa managedin stance-patch-compliance-sta tus	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 20.2	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.
Seni 20.2	vuln-management-plan-exists (Pemeriksaan Proses)	Pastikan rencana manajemen kerentanan dikembangkan dan diimplementasikan untuk memiliki proses yang ditentukan secara formal untuk mengatasi kerentanan di lingkungan Anda. Ini dapat mencakup alat manajemen kerentanan, irama pemindaian lingkungan, peran dan tanggung jawab.
Seni. 21.1	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	ec2- ebs-encryption-by-default	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Seni. 21.1	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.
Seni. 21.1	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
Seni. 21.1	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Seni. 21.1	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Seni. 21.1	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Seni. 21.1	sns-encrypted-kms	Untuk membantu melindung i data saat istirahat, pastikan topik Amazon Simple Notificat ion Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	alb-http-to-https-pengalihan-periksa	Untuk membantu melindung i data dalam perjalanan, pastikan bahwa Applicati on Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Seni. 21.1	api-gw-cache-enabled-dan-di enkripsi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Seni. 21.1	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifika t SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
Seni. 21.1	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.
Seni. 21.1	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.
Seni. 21.1	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
Seni. 21.1	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
Seni. 21.1	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
Seni. 21.1	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
Seni. 21.1	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) menyediakan ketersediaan dan daya tahan yang ditingkatkan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	rds-cluster-multi-az-diaktifkan	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) menyediakan ketersediaan dan daya tahan yang ditingkatkan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	rds-storage-encrypted	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Seni. 21.1	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastika n bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberika n informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	redshift-cluster-kms-enabled	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Seni. 21.1	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerluka n enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Seni. 21.1	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	s3- bucket-ssl-requests-only	Untuk membantu melindung i data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerluka n permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Seni. 21.1	sagemaker-endpoint-configur ation-kms-kunci-dikonfigurasi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 21.1	secretsmanager-using-cmk	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Seni. 21.1	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimpleme ntasikan untuk mencapai persyaratan ketahanan . Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-S ite VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
Seni 22	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
Seni 22	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspo s informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
Seni 22	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
Seni 22	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearc h Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
Seni 22	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkin kan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabk an akses tidak sah ke sumber daya VPC Amazon.
Seni 22	lambda-function-public-acce ss-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyarat an untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearc h Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
Seni 22	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
Seni 22	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,338 9,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
Seni 22	s3- -dilarang bucket-level-publi c-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
Seni 22	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
Seni 22	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
Seni 22	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 22	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.
Seni 23	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 23	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimk an file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 23	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
Seni 23	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
Seni 23	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 23	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
Seni 23	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
Seni 23	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 23	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.
Seni 23	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni 23	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.
Seni 23	vpc-flow-logs-enabled	Log aliran VPC menyediak an catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 24.2	response-plan-exists-maintained (Pemeriksaan Proses)	Memastikan rencana respons insiden dibuat, dipelihara, dan didistribusikan kepada personel yang bertanggung jawab. Memiliki rencana respons yang diperbarui dan didokumentasikan secara formal dapat membantu memastikan personel respons memahami peran, tanggung jawab, dan proses yang harus diikuti selama insiden.
Seni. 24.1	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 25	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
Seni. 25	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 25	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
Seni. 25	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relational Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 25	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.
Seni. 25	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 25	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan cadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.
Seni. 25	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediak an kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 25	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.
Seni. 25	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	AWS Aturan Config	Bimbingan
Seni. 25	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihka n setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

Templat

Template ini tersedia di GitHub: Praktik Terbaik Operasional untuk Esquema Nacional de Seguridad (ENS) Tinggi.

Praktik Terbaik Operasional untuk FDA Judul 21 CFR Bagian 11

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara Judul 21 dari Kode Peraturan Federal (CFR) Bagian 11 dan aturan AWS Config terkelola. Setiap AWS Config aturan berlaku untuk AWS sumber daya

tertentu, dan berkaitan dengan satu atau lebih kontrol FDA Title 21 CFR Bagian 11. Kontrol FDA Title 21 CFR Part 11 dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.1	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut:	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.
11.1	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara,	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integrita s, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandata ngani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut:		adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.1	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut:	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.1	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut:	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.1	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut:	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.1	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut:	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.1	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut:	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.1	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut:	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relational Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.1	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut:	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.1	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut:	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.1	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut:	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (a)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (a) Validasi sistem untuk memastikan akurasi, keandalan, kinerja yang dimaksudkan secara konsisten, dan kemampuan untuk membedakan catatan yang tidak valid atau diubah.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup Anda diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (a)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (a) Validasi sistem untuk memastikan akurasi, keandalan, kinerja yang dimaksudkan secara konsisten, dan kemampuan untuk membedakan catatan yang tidak valid atau diubah.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (a)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (a) Validasi sistem untuk memastikan akurasi, keandalan, kinerja yang dimaksudkan secara konsisten, dan kemampuan untuk membedakan catatan yang tidak valid atau diubah.	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (a)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (a) Validasi sistem untuk memastikan akurasi, keandalan, kinerja yang dimaksudkan secara konsisten, dan kemampuan untuk membedakan catatan yang tidak valid atau diubah.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus, atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (a)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (a) Validasi sistem untuk memastikan akurasi, keandalan, kinerja yang dimaksudkan secara konsisten, dan kemampuan untuk membedakan catatan yang tidak valid atau diubah.	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (a)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (a) Validasi sistem untuk memastikan akurasi, keandalan, kinerja yang dimaksudkan secara konsisten, dan kemampuan untuk membedakan catatan yang tidak valid atau diubah.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (a)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (a) Validasi sistem untuk memastikan akurasi, keandalan, kinerja yang dimaksudkan secara konsisten, dan kemampuan untuk membedakan catatan yang tidak valid atau diubah.	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (a)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (a) Validasi sistem untuk memastikan akurasi, keandalan, kinerja yang dimaksudkan secara konsisten, dan kemampuan untuk membedakan catatan yang tidak valid atau diubah.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (a)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (a) Validasi sistem untuk memastikan akurasi, keandalan, kinerja yang dimaksudkan secara konsisten, dan kemampuan untuk membedakan catatan yang tidak valid atau diubah.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (a)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (a) Validasi sistem untuk memastikan akurasi, keandalan, kinerja yang dimaksudkan secara konsisten, dan kemampuan untuk membedakan catatan yang tidak valid atau diubah.	dynamodb-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (a)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (a) Validasi sistem untuk memastikan akurasi, keandalan, kinerja yang dimaksudkan secara konsisten, dan kemampuan untuk membedakan catatan yang tidak valid atau diubah.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (a)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (a) Validasi sistem untuk memastikan akurasi, keandalan, kinerja yang dimaksudkan secara konsisten, dan kemampuan untuk membedakan catatan yang tidak valid atau diubah.	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (a)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (a) Validasi sistem untuk memastikan akurasi, keandalan, kinerja yang dimaksudkan secara konsisten, dan kemampuan untuk membedakan catatan yang tidak valid atau diubah.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (a)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (a) Validasi sistem untuk memastikan akurasi, keandalan, kinerja yang dimaksudkan secara konsisten, dan kemampuan untuk membedakan catatan yang tidak valid atau diubah.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (a)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (a) Validasi sistem untuk memastikan akurasi, keandalan, kinerja yang dimaksudkan secara konsisten, dan kemampuan untuk membedakan catatan yang tidak valid atau diubah.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (a)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (a) Validasi sistem untuk memastikan akurasi, keandalan, kinerja yang dimaksudkan secara konsisten, dan kemampuan untuk membedakan catatan yang tidak valid atau diubah.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (a)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (a) Validasi sistem untuk memastikan akurasi, keandalan, kinerja yang dimaksudkan secara konsisten, dan kemampuan untuk membedakan catatan yang tidak valid atau diubah.	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (a)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (a) Validasi sistem untuk memastikan akurasi, keandalan, kinerja yang dimaksudkan secara konsisten, dan kemampuan untuk membedakan catatan yang tidak valid atau diubah.	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (a)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (a) Validasi sistem untuk memastikan akurasi, keandalan, kinerja yang dimaksudkan secara konsisten, dan kemampuan untuk membedakan catatan yang tidak valid atau diubah.	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (a)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (a) Validasi sistem untuk memastikan akurasi, keandalan, kinerja yang dimaksudkan secara konsisten, dan kemampuan untuk membedakan catatan yang tidak valid atau diubah.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (a)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (a) Validasi sistem untuk memastikan akurasi, keandalan, kinerja yang dimaksudkan secara konsisten, dan kemampuan untuk membedakan catatan yang tidak valid atau diubah.	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (a)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (a) Validasi sistem untuk memastikan akurasi, keandalan, kinerja yang dimaksudkan secara konsisten, dan kemampuan untuk membedakan catatan yang tidak valid atau diubah.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (a)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (a) Validasi sistem untuk memastikan akurasi, keandalan, kinerja yang dimaksudkan secara konsisten, dan kemampuan untuk membedakan catatan yang tidak valid atau diubah.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relational Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (a)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (a) Validasi sistem untuk memastikan akurasi, keandalan, kinerja yang dimaksudkan secara konsisten, dan kemampuan untuk membedakan catatan yang tidak valid atau diubah.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) menyediakan ketersediaan dan daya tahan yang ditingkatkan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (a)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (a) Validasi sistem untuk memastikan akurasi, keandalan, kinerja yang dimaksudkan secara konsisten, dan kemampuan untuk membedakan catatan yang tidak valid atau diubah.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (a)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (a) Validasi sistem untuk memastikan akurasi, keandalan, kinerja yang dimaksudkan secara konsisten, dan kemampuan untuk membedakan catatan yang tidak valid atau diubah.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (a)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (a) Validasi sistem untuk memastikan akurasi, keandalan, kinerja yang dimaksudkan secara konsisten, dan kemampuan untuk membedakan catatan yang tidak valid atau diubah.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (a)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (a) Validasi sistem untuk memastikan akurasi, keandalan, kinerja yang dimaksudkan secara konsisten, dan kemampuan untuk membedakan catatan yang tidak valid atau diubah.	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (c)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (c) Perlindungan catatan untuk memungkinkan pengambilan yang akurat dan siap selama periode penyimpanan catatan.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (c)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (c) Perlindungan catatan untuk memungkinkan pengambilan yang akurat dan siap selama periode penyimpanan catatan.	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (c)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (c) Perlindungan catatan untuk memungkinkan pengambilan yang akurat dan siap selama periode penyimpanan catatan.	ecr-private-lifecycle-policy-dikonfigurasi	Kebijakan siklus hidup Amazon Elastic Container Repository (ECR) memungkinkan Anda menentukan manajemen siklus hidup gambar dalam repositori. Ini memungkinkan otomatisasi membersihkan gambar yang tidak digunakan, seperti gambar kedaluwarsa berdasarkan usia atau hitungan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (c)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (c) Perlindungan catatan untuk memungkinkan pengambilan yang akurat dan siap selama periode penyimpanan catatan.	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (c)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (c) Perlindungan catatan untuk memungkinkan pengambilan yang akurat dan siap selama periode penyimpanan catatan.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (c)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (c) Perlindungan catatan untuk memungkinkan pengambilan yang akurat dan siap selama periode penyimpanan catatan.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (c)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (c) Perlindungan catatan untuk memungkinkan pengambilan yang akurat dan siap selama periode penyimpanan catatan.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (c)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (c) Perlindungan catatan untuk memungkinkan pengambilan yang akurat dan siap selama periode penyimpanan catatan.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (c)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (c) Perlindungan catatan untuk memungkinkan pengambilan yang akurat dan siap selama periode penyimpanan catatan.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (c)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (c) Perlindungan catatan untuk memungkinkan pengambilan yang akurat dan siap selama periode penyimpanan catatan.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (c)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (c) Perlindungan catatan untuk memungkinkan pengambilan yang akurat dan siap selama periode penyimpanan catatan.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (c)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (c) Perlindungan catatan untuk memungkinkan pengambilan yang akurat dan siap selama periode penyimpanan catatan.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (c)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (c) Perlindungan catatan untuk memungkinkan pengambilan yang akurat dan siap selama periode penyimpanan catatan.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (c)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (c) Perlindungan catatan untuk memungkinkan pengambilan yang akurat dan siap selama periode penyimpanan catatan.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (c)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (c) Perlindungan catatan untuk memungkinkan pengambilan yang akurat dan siap selama periode penyimpanan catatan.	s3- version-lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihkan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (c)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (c) Perlindungan catatan untuk memungkinkan pengambilan yang akurat dan siap selama periode penyimpanan catatan.	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (c)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (c) Perlindungan catatan untuk memungkinkan pengambilan yang akurat dan siap selama periode penyimpanan catatan.	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (c)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (c) Perlindungan catatan untuk memungkinkan pengambilan yang akurat dan siap selama periode penyimpanan catatan.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktifkan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediakan sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi, pengembalian, dan pendelegasian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigurasi ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	secretsmanager-rotation-enabled-check	Aturan ini memastikan AWS rahasia Secrets Manager telah diaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	secretsmanager-scheduled-rotation-success-periksa	Aturan ini memastikan bahwa AWS rahasia Secrets Manager telah berhasil diputar sesuai dengan jadwal rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode di mana rahasia aktif, dan berpotensi mengurangi dampak bisnis jika dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (d)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (d) Membatasi akses sistem ke individu yang berwenang.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (e)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (e) Penggunaan jejak audit yang aman, dihasilkan komputer, dan dicap waktu untuk mencatat secara independen tanggal dan waktu entri dan tindakan operator yang	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	membuat, memodifikasi, atau menghapus catatan elektronik. Perubahan catatan tidak akan mengaburkan informasi yang direkam sebelumnya. Dokumentasi jejak audit tersebut harus disimpan untuk jangka waktu setidaknya selama yang diperlukan untuk catatan elektronik subjek dan harus tersedia untuk peninjauan dan penyalinan agensi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (e)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (e) Penggunaan jejak audit yang aman, dihasilkan komputer, dan dicap waktu untuk mencatat secara independen tanggal dan waktu entri dan tindakan operator yang	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	membuat, memodifikasi, atau menghapus catatan elektronik. Perubahan catatan tidak akan mengaburkan informasi yang direkam sebelumnya. Dokumentasi jejak audit tersebut harus disimpan untuk jangka waktu setidaknya selama yang diperlukan untuk catatan elektronik subjek dan harus tersedia untuk peninjauan dan penyalinan agensi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (e)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (e) Penggunaan jejak audit yang aman, dihasilkan komputer, dan dicap waktu untuk mencatat secara independen tanggal dan waktu entri dan tindakan operator yang	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	membuat, memodifikasi, atau menghapus catatan elektronik. Perubahan catatan tidak akan mengaburkan informasi yang direkam sebelumnya. Dokumentasi jejak audit tersebut harus disimpan untuk jangka waktu setidaknya selama yang diperlukan untuk catatan elektronik subjek dan harus tersedia untuk peninjauan dan penyalinan agensi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (e)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (e) Penggunaan jejak audit yang aman, dihasilkan komputer, dan dicap waktu untuk mencatat secara independen tanggal dan waktu entri dan tindakan operator yang	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	membuat, memodifikasi, atau menghapus catatan elektronik. Perubahan catatan tidak akan mengaburkan informasi yang direkam sebelumnya. Dokumentasi jejak audit tersebut harus disimpan untuk jangka waktu setidaknya selama yang diperlukan untuk catatan elektronik subjek dan harus tersedia untuk peninjauan dan penyalinan agensi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (e)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (e) Penggunaan jejak audit yang aman, dihasilkan komputer, dan dicap waktu untuk mencatat secara independen tanggal dan waktu entri dan tindakan operator yang	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	membuat, memodifikasi, atau menghapus catatan elektronik. Perubahan catatan tidak akan mengaburkan informasi yang direkam sebelumnya. Dokumentasi jejak audit tersebut harus disimpan untuk jangka waktu setidaknya selama yang diperlukan untuk catatan elektronik subjek dan harus tersedia untuk peninjauan dan penyalinan agensi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (e)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (e) Penggunaan jejak audit yang aman, dihasilkan komputer, dan dicap waktu untuk mencatat secara independen tanggal dan waktu entri dan tindakan operator yang	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	membuat, memodifikasi, atau menghapus catatan elektronik. Perubahan catatan tidak akan mengaburkan informasi yang direkam sebelumnya. Dokumentasi jejak audit tersebut harus disimpan untuk jangka waktu setidaknya selama yang diperlukan untuk catatan elektronik subjek dan harus tersedia untuk peninjauan dan penyalinan agensi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (e)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (e) Penggunaan jejak audit yang aman, dihasilkan komputer, dan dicap waktu untuk mencatat secara independen tanggal dan waktu entri dan tindakan operator yang	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	membuat, memodifikasi, atau menghapus catatan elektronik. Perubahan catatan tidak akan mengaburkan informasi yang direkam sebelumnya. Dokumentasi jejak audit tersebut harus disimpan untuk jangka waktu setidaknya selama yang diperlukan untuk catatan elektronik subjek dan harus tersedia untuk peninjauan dan penyalinan agensi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (e)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (e) Penggunaan jejak audit yang aman, dihasilkan komputer, dan dicap waktu untuk mencatat secara independen tanggal dan waktu entri dan tindakan operator yang	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	membuat, memodifikasi, atau menghapus catatan elektronik. Perubahan catatan tidak akan mengaburkan informasi yang direkam sebelumnya. Dokumentasi jejak audit tersebut harus disimpan untuk jangka waktu setidaknya selama yang diperlukan untuk catatan elektronik subjek dan harus tersedia untuk peninjauan dan penyalinan agensi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (e)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (e) Penggunaan jejak audit yang aman, dihasilkan komputer, dan dicap waktu untuk mencatat secara independen tanggal dan waktu entri dan tindakan operator yang	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	membuat, memodifikasi, atau menghapus catatan elektronik. Perubahan catatan tidak akan mengaburkan informasi yang direkam sebelumnya. Dokumentasi jejak audit tersebut harus disimpan untuk jangka waktu setidaknya selama yang diperlukan untuk catatan elektronik subjek dan harus tersedia untuk peninjauan dan penyalinan agensi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (e)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (e) Penggunaan jejak audit yang aman, dihasilkan komputer, dan dicap waktu untuk mencatat secara independen tanggal dan waktu entri dan tindakan operator yang	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktifkan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediakan sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	membuat, memodifikasi, atau menghapus catatan elektronik. Perubahan catatan tidak akan mengaburkan informasi yang direkam sebelumnya. Dokumentasi jejak audit tersebut harus disimpan untuk jangka waktu setidaknya selama yang diperlukan untuk catatan elektronik subjek dan harus tersedia untuk peninjauan dan penyalinan agensi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (e)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (e) Penggunaan jejak audit yang aman, dihasilkan komputer, dan dicap waktu untuk mencatat secara independen tanggal dan waktu entri dan tindakan operator yang	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	membuat, memodifikasi, atau menghapus catatan elektronik. Perubahan catatan tidak akan mengaburkan informasi yang direkam sebelumnya. Dokumentasi jejak audit tersebut harus disimpan untuk jangka waktu setidaknya selama yang diperlukan untuk catatan elektronik subjek dan harus tersedia untuk peninjauan dan penyalinan agensi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (e)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (e) Penggunaan jejak audit yang aman, dihasilkan komputer, dan dicap waktu untuk mencatat secara independen tanggal dan waktu entri dan tindakan operator yang	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	membuat, memodifikasi, atau menghapus catatan elektronik. Perubahan catatan tidak akan mengaburkan informasi yang direkam sebelumnya. Dokumentasi jejak audit tersebut harus disimpan untuk jangka waktu setidaknya selama yang diperlukan untuk catatan elektronik subjek dan harus tersedia untuk peninjauan dan penyalinan agensi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (e)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (e) Penggunaan jejak audit yang aman, dihasilkan komputer, dan dicap waktu untuk mencatat secara independen tanggal dan waktu entri dan tindakan operator yang	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	membuat, memodifikasi, atau menghapus catatan elektronik. Perubahan catatan tidak akan mengaburkan informasi yang direkam sebelumnya. Dokumentasi jejak audit tersebut harus disimpan untuk jangka waktu setidaknya selama yang diperlukan untuk catatan elektronik subjek dan harus tersedia untuk peninjauan dan penyalinan agensi.		(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (e)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (e) Penggunaan jejak audit yang aman, dihasilkan komputer, dan dicap waktu untuk mencatat secara independen tanggal dan waktu entri dan tindakan operator yang	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	membuat, memodifikasi, atau menghapus catatan elektronik. Perubahan catatan tidak akan mengaburkan informasi yang direkam sebelumnya. Dokumentasi jejak audit tersebut harus disimpan untuk jangka waktu setidaknya selama yang diperlukan untuk catatan elektronik subjek dan harus tersedia untuk peninjauan dan penyalinan agensi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (e)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (e) Penggunaan jejak audit yang aman, dihasilkan komputer, dan dicap waktu untuk mencatat secara independen tanggal dan waktu entri dan tindakan operator yang	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	membuat, memodifikasi, atau menghapus catatan elektronik. Perubahan catatan tidak akan mengaburkan informasi yang direkam sebelumnya. Dokumentasi jejak audit tersebut harus disimpan untuk jangka waktu setidaknya selama yang diperlukan untuk catatan elektronik subjek dan harus tersedia untuk peninjauan dan penyalinan agensi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (e)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (e) Penggunaan jejak audit yang aman, dihasilkan komputer, dan dicap waktu untuk mencatat secara independen tanggal dan waktu entri dan tindakan operator yang	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	membuat, memodifikasi, atau menghapus catatan elektronik. Perubahan catatan tidak akan mengaburkan informasi yang direkam sebelumnya. Dokumentasi jejak audit tersebut harus disimpan untuk jangka waktu setidaknya selama yang diperlukan untuk catatan elektronik subjek dan harus tersedia untuk peninjauan dan penyalinan agensi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (e)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (e) Penggunaan jejak audit yang aman, dihasilkan komputer, dan dicap waktu untuk mencatat secara independen tanggal dan waktu entri dan tindakan operator yang	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	membuat, memodifikasi, atau menghapus catatan elektronik. Perubahan catatan tidak akan mengaburkan informasi yang direkam sebelumnya. Dokumentasi jejak audit tersebut harus disimpan untuk jangka waktu setidaknya selama yang diperlukan untuk catatan elektronik subjek dan harus tersedia untuk peninjauan dan penyalinan agensi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (e)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (e) Penggunaan jejak audit yang aman, dihasilkan komputer, dan dicap waktu untuk mencatat secara independen tanggal dan waktu entri dan tindakan operator yang	redshift-audit-logging-enabled	Untuk menangkap informasi tentang koneksi dan aktivitas pengguna di klaster Amazon Redshift, pastikan pencatatan audit diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	membuat, memodifikasi, atau menghapus catatan elektronik. Perubahan catatan tidak akan mengaburkan informasi yang direkam sebelumnya. Dokumentasi jejak audit tersebut harus disimpan untuk jangka waktu setidaknya selama yang diperlukan untuk catatan elektronik subjek dan harus tersedia untuk peninjauan dan penyalinan agensi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (e)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (e) Penggunaan jejak audit yang aman, dihasilkan komputer, dan dicap waktu untuk mencatat secara independen tanggal dan waktu entri dan tindakan operator yang	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	membuat, memodifikasi, atau menghapus catatan elektronik. Perubahan catatan tidak akan mengaburkan informasi yang direkam sebelumnya. Dokumentasi jejak audit tersebut harus disimpan untuk jangka waktu setidaknya selama yang diperlukan untuk catatan elektronik subjek dan harus tersedia untuk peninjauan dan penyalinan agensi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (e)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (e) Penggunaan jejak audit yang aman, dihasilkan komputer, dan dicap waktu untuk mencatat secara independen tanggal dan waktu entri dan tindakan operator yang	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	membuat, memodifikasi, atau menghapus catatan elektronik. Perubahan catatan tidak akan mengaburkan informasi yang direkam sebelumnya. Dokumentasi jejak audit tersebut harus disimpan untuk jangka waktu setidaknya selama yang diperlukan untuk catatan elektronik subjek dan harus tersedia untuk peninjauan dan penyalinan agensi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (e)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (e) Penggunaan jejak audit yang aman, dihasilkan komputer, dan dicap waktu untuk mencatat secara independen tanggal dan waktu entri dan tindakan operator yang	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	membuat, memodifikasi, atau menghapus catatan elektronik. Perubahan catatan tidak akan mengaburkan informasi yang direkam sebelumnya. Dokumentasi jejak audit tersebut harus disimpan untuk jangka waktu setidaknya selama yang diperlukan untuk catatan elektronik subjek dan harus tersedia untuk peninjauan dan penyalinan agensi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (e)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (e) Penggunaan jejak audit yang aman, dihasilkan komputer, dan dicap waktu untuk mencatat secara independen tanggal dan waktu entri dan tindakan operator yang	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	membuat, memodifikasi, atau menghapus catatan elektronik. Perubahan catatan tidak akan mengaburkan informasi yang direkam sebelumnya. Dokumentasi jejak audit tersebut harus disimpan untuk jangka waktu setidaknya selama yang diperlukan untuk catatan elektronik subjek dan harus tersedia untuk peninjauan dan penyalinan agensi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktifkan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediakan sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi, pengembalian, dan pendelegasian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePreve ntion MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigurasi ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositori data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	secretsmanager-rotation-enabled-check	Aturan ini memastikan AWS rahasia Secrets Manager telah diaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	secretsmanager-scheduled-rotation-success-periksa	Aturan ini memastikan bahwa AWS rahasia Secrets Manager telah berhasil diputar sesuai dengan jadwal rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode di mana rahasia aktif, dan berpotensi mengurangi dampak bisnis jika dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (g)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (g) Penggunaan pemeriksaan otoritas untuk memastikan bahwa hanya individu yang berwenang yang dapat menggunakan sistem, menandatangani catatan secara elektronik,	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengakses operasi atau perangkat input atau output sistem komputer, mengubah catatan, atau melakukan operasi yang ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (h)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (h) Penggunaan perangkat (misalnya, terminal) pemeriksaan untuk menentukan, jika sesuai, validitas sumber input data atau instruksi operasional.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (h)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (h) Penggunaan perangkat (misalnya, terminal) pemeriksaan untuk menentukan, jika sesuai, validitas sumber input data atau instruksi operasional.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (h)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (h) Penggunaan perangkat (misalnya, terminal) pemeriksaan untuk menentukan, jika sesuai, validitas sumber input data atau instruksi operasional.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (i)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut mencakup hal-hal berikut: (i) Penentuan bahwa orang yang mengembangkan, memelihara, atau menggunakan sistem catatan elektronik/tanda tangan elektronik memiliki pendidikan, pelatihan, dan pengalaman untuk	security-awareness-program-exists (pemeriksaan proses)	Membangun dan memelihara program kesadaran keamanan untuk organisasi Anda. Program kesadaran keamanan mendidik karyawan tentang cara melindungi organisasi mereka dari berbagai pelanggaran atau insiden keamanan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	melakukan tugas yang ditugaskan.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (k)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (k) Penggunaan kontrol yang tepat atas dokumentasi sistem termasuk: (1) Kontrol yang memadai atas distribusi, akses ke, dan penggunaan dokumentasi untuk pengoperasian	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan pemeliharaan sistem. (2) Revisi dan prosedur pengendal ian perubahan untuk mempertah ankan jejak audit yang mendokume ntasikan pengemban gan dan modifikasi dokumentasi sistem yang diurutkan waktu.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (k)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (k) Penggunaan kontrol yang tepat atas dokumentasi sistem termasuk: (1) Kontrol yang memadai atas distribusi, akses ke, dan penggunaan dokumentasi untuk pengoperasian	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan pemeliharaan sistem. (2) Revisi dan prosedur pengendal ian perubahan untuk mempertah ankan jejak audit yang mendokume ntasikan pengemban gan dan modifikasi dokumentasi sistem yang diurutkan waktu.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (k)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (k) Penggunaan kontrol yang tepat atas dokumentasi sistem termasuk: (1) Kontrol yang memadai atas distribusi, akses ke, dan penggunaan dokumentasi untuk pengoperasian	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan pemeliharaan sistem. (2) Revisi dan prosedur pengendal ian perubahan untuk mempertah ankan jejak audit yang mendokume ntasikan pengemban gan dan modifikasi dokumentasi sistem yang diurutkan waktu.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (k)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (k) Penggunaan kontrol yang tepat atas dokumentasi sistem termasuk: (1) Kontrol yang memadai atas distribusi, akses ke, dan penggunaan dokumentasi untuk pengoperasian	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan pemeliharaan sistem. (2) Revisi dan prosedur pengendal ian perubahan untuk mempertah ankan jejak audit yang mendokume ntasikan pengemban gan dan modifikasi dokumentasi sistem yang diurutkan waktu.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (k)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (k) Penggunaan kontrol yang tepat atas dokumentasi sistem termasuk: (1) Kontrol yang memadai atas distribusi, akses ke, dan penggunaan dokumentasi untuk pengoperasian	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan pemeliharaan sistem. (2) Revisi dan prosedur pengendal ian perubahan untuk mempertah ankan jejak audit yang mendokume ntasikan pengemban gan dan modifikasi dokumentasi sistem yang diurutkan waktu.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (k)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (k) Penggunaan kontrol yang tepat atas dokumentasi sistem termasuk: (1) Kontrol yang memadai atas distribusi, akses ke, dan penggunaan dokumentasi untuk pengoperasian	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan pemeliharaan sistem. (2) Revisi dan prosedur pengendal ian perubahan untuk mempertah ankan jejak audit yang mendokume ntasikan pengemban gan dan modifikasi dokumentasi sistem yang diurutkan waktu.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (k)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (k) Penggunaan kontrol yang tepat atas dokumentasi sistem termasuk: (1) Kontrol yang memadai atas distribusi, akses ke, dan penggunaan dokumentasi untuk pengoperasian	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan pemeliharaan sistem. (2) Revisi dan prosedur pengendal ian perubahan untuk mempertah ankan jejak audit yang mendokume ntasikan pengemban gan dan modifikasi dokumentasi sistem yang diurutkan waktu.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (k)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (k) Penggunaan kontrol yang tepat atas dokumentasi sistem termasuk: (1) Kontrol yang memadai atas distribusi, akses ke, dan penggunaan dokumentasi untuk pengoperasian	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan pemeliharaan sistem. (2) Revisi dan prosedur pengendal ian perubahan untuk mempertah ankan jejak audit yang mendokume ntasikan pengemban gan dan modifikasi dokumentasi sistem yang diurutkan waktu.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (k)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (k) Penggunaan kontrol yang tepat atas dokumentasi sistem termasuk: (1) Kontrol yang memadai atas distribusi, akses ke, dan penggunaan dokumentasi untuk pengoperasian	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan pemeliharaan sistem. (2) Revisi dan prosedur pengendal ian perubahan untuk mempertah ankan jejak audit yang mendokume ntasikan pengemban gan dan modifikasi dokumentasi sistem yang diurutkan waktu.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (k)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (k) Penggunaan kontrol yang tepat atas dokumentasi sistem termasuk: (1) Kontrol yang memadai atas distribusi, akses ke, dan penggunaan dokumentasi untuk pengoperasian	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan pemeliharaan sistem. (2) Revisi dan prosedur pengendal ian perubahan untuk mempertah ankan jejak audit yang mendokume ntasikan pengemban gan dan modifikasi dokumentasi sistem yang diurutkan waktu.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (k)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (k) Penggunaan kontrol yang tepat atas dokumentasi sistem termasuk: (1) Kontrol yang memadai atas distribusi, akses ke, dan penggunaan dokumentasi untuk pengoperasian	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan pemeliharaan sistem. (2) Revisi dan prosedur pengendal ian perubahan untuk mempertah ankan jejak audit yang mendokume ntasikan pengemban gan dan modifikasi dokumentasi sistem yang diurutkan waktu.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (k)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (k) Penggunaan kontrol yang tepat atas dokumentasi sistem termasuk: (1) Kontrol yang memadai atas distribusi, akses ke, dan penggunaan dokumentasi untuk pengoperasian	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan pemeliharaan sistem. (2) Revisi dan prosedur pengendal ian perubahan untuk mempertah ankan jejak audit yang mendokume ntasikan pengemban gan dan modifikasi dokumentasi sistem yang diurutkan waktu.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (k)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (k) Penggunaan kontrol yang tepat atas dokumentasi sistem termasuk: (1) Kontrol yang memadai atas distribusi, akses ke, dan penggunaan dokumentasi untuk pengoperasian	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan pemeliharaan sistem. (2) Revisi dan prosedur pengendal ian perubahan untuk mempertah ankan jejak audit yang mendokume ntasikan pengemban gan dan modifikasi dokumentasi sistem yang diurutkan waktu.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (k)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (k) Penggunaan kontrol yang tepat atas dokumentasi sistem termasuk: (1) Kontrol yang memadai atas distribusi, akses ke, dan penggunaan dokumentasi untuk pengoperasian	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan pemeliharaan sistem. (2) Revisi dan prosedur pengendal ian perubahan untuk mempertah ankan jejak audit yang mendokume ntasikan pengemban gan dan modifikasi dokumentasi sistem yang diurutkan waktu.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (k)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (k) Penggunaan kontrol yang tepat atas dokumentasi sistem termasuk: (1) Kontrol yang memadai atas distribusi, akses ke, dan penggunaan dokumentasi untuk pengoperasian	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan pemeliharaan sistem. (2) Revisi dan prosedur pengendal ian perubahan untuk mempertah ankan jejak audit yang mendokume ntasikan pengemban gan dan modifikasi dokumentasi sistem yang diurutkan waktu.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (k)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (k) Penggunaan kontrol yang tepat atas dokumentasi sistem termasuk: (1) Kontrol yang memadai atas distribusi, akses ke, dan penggunaan dokumentasi untuk pengoperasian	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan pemeliharaan sistem. (2) Revisi dan prosedur pengendal ian perubahan untuk mempertah ankan jejak audit yang mendokume ntasikan pengemban gan dan modifikasi dokumentasi sistem yang diurutkan waktu.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (k)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (k) Penggunaan kontrol yang tepat atas dokumentasi sistem termasuk: (1) Kontrol yang memadai atas distribusi, akses ke, dan penggunaan dokumentasi untuk pengoperasian	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan pemeliharaan sistem. (2) Revisi dan prosedur pengendal ian perubahan untuk mempertah ankan jejak audit yang mendokume ntasikan pengemban gan dan modifikasi dokumentasi sistem yang diurutkan waktu.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (k)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (k) Penggunaan kontrol yang tepat atas dokumentasi sistem termasuk: (1) Kontrol yang memadai atas distribusi, akses ke, dan penggunaan dokumentasi untuk pengoperasian	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan pemeliharaan sistem. (2) Revisi dan prosedur pengendal ian perubahan untuk mempertah ankan jejak audit yang mendokume ntasikan pengemban gan dan modifikasi dokumentasi sistem yang diurutkan waktu.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (k)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (k) Penggunaan kontrol yang tepat atas dokumentasi sistem termasuk: (1) Kontrol yang memadai atas distribusi, akses ke, dan penggunaan dokumentasi untuk pengoperasian	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan pemeliharaan sistem. (2) Revisi dan prosedur pengendal ian perubahan untuk mempertah ankan jejak audit yang mendokume ntasikan pengemban gan dan modifikasi dokumentasi sistem yang diurutkan waktu.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (k)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (k) Penggunaan kontrol yang tepat atas dokumentasi sistem termasuk: (1) Kontrol yang memadai atas distribusi, akses ke, dan penggunaan dokumentasi untuk pengoperasian	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan pemeliharaan sistem. (2) Revisi dan prosedur pengendal ian perubahan untuk mempertah ankan jejak audit yang mendokume ntasikan pengemban gan dan modifikasi dokumentasi sistem yang diurutkan waktu.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (k)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (k) Penggunaan kontrol yang tepat atas dokumentasi sistem termasuk: (1) Kontrol yang memadai atas distribusi, akses ke, dan penggunaan dokumentasi untuk pengoperasian	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan pemeliharaan sistem. (2) Revisi dan prosedur pengendal ian perubahan untuk mempertah ankan jejak audit yang mendokume ntasikan pengemban gan dan modifikasi dokumentasi sistem yang diurutkan waktu.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.10 (k)	Orang yang menggunakan sistem tertutup untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, bila perlu, kerahasiaan catatan elektronik, dan untuk memastikan bahwa penandatangan tidak dapat dengan mudah menolak catatan yang ditandatangani sebagai tidak asli. Prosedur dan kontrol tersebut harus mencakup hal-hal berikut: (k) Penggunaan kontrol yang tepat atas dokumentasi sistem termasuk: (1) Kontrol yang memadai atas distribusi, akses ke, dan penggunaan dokumentasi untuk pengoperasian	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan pemeliharaan sistem. (2) Revisi dan prosedur pengendal ian perubahan untuk mempertah ankan jejak audit yang mendokume ntasikan pengemban gan dan modifikasi dokumentasi sistem yang diurutkan waktu.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	(a) Tanda tangan elektronik yang tidak didasarkan pada biometrik harus: (1) Menggunakan setidaknya dua komponen identifikasi yang berbeda seperti kode identifikasi dan kata sandi. (i) Ketika seorang individu mengeksekusi serangkaian penandatanganan selama satu periode akses sistem terkontrol yang berkelanjutan, penandatanganan pertama harus dijalankan menggunakan semua komponen tanda tangan elektronik; penandatanganan berikutnya harus dijalankan menggunakan setidaknya satu komponen tanda tangan elektronik yang hanya dapat dieksekusi oleh, dan dirancang untuk	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	digunakan hanya oleh, individu. (ii) Ketika seorang individu mengeksek usi satu atau lebih penandatanganan yang tidak dilakukan selama satu periode akses sistem terkontrol yang berkelanjutan, setiap penandatanganan harus dijalankan menggunakan semua komponen tanda tangan elektronik. (2) Digunakan hanya oleh pemilik asli mereka; dan (3) Dikelola dan dilaksanakan untuk memastikan bahwa upaya penggunaan tanda tangan elektroni k individu oleh siapa pun selain pemilik aslinya memerlukan kolaborasi dua orang atau lebih.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	(a) Tanda tangan elektronik yang tidak didasarkan pada biometrik harus: (1) Menggunakan setidaknya dua komponen identifikasi yang berbeda seperti kode identifikasi dan kata sandi. (i) Ketika seorang individu mengeksekusi serangkaian penandatanganan selama satu periode akses sistem terkontrol yang berkelanjutan, penandatanganan pertama harus dijalankan menggunakan semua komponen tanda tangan elektronik; penandatanganan berikutnya harus dijalankan menggunakan setidaknya satu komponen tanda tangan elektronik yang hanya dapat dieksekusi oleh, dan dirancang untuk	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	digunakan hanya oleh, individu. (ii) Ketika seorang individu mengeksek usi satu atau lebih penandatanganan yang tidak dilakukan selama satu periode akses sistem terkontrol yang berkelanjutan, setiap penandatanganan harus dijalankan menggunakan semua komponen tanda tangan elektronik. (2) Digunakan hanya oleh pemilik asli mereka; dan (3) Dikelola dan dilaksanakan untuk memastikan bahwa upaya penggunaan tanda tangan elektroni k individu oleh siapa pun selain pemilik aslinya memerlukan kolaborasi dua orang atau lebih.		(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePreve ntion MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	(a) Tanda tangan elektronik yang tidak didasarkan pada biometrik harus: (1) Menggunakan setidaknya dua komponen identifikasi yang berbeda seperti kode identifikasi dan kata sandi. (i) Ketika seorang individu mengeksekusi serangkaian penandatanganan selama satu periode akses sistem terkontrol yang berkelanjutan, penandatanganan pertama harus dijalankan menggunakan semua komponen tanda tangan elektronik; penandatanganan berikutnya harus dijalankan menggunakan setidaknya satu komponen tanda tangan elektronik yang hanya dapat dieksekusi oleh, dan dirancang untuk	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	digunakan hanya oleh, individu. (ii) Ketika seorang individu mengeksek usi satu atau lebih penandatanganan yang tidak dilakukan selama satu periode akses sistem terkontrol yang berkelanjutan, setiap penandatanganan harus dijalankan menggunakan semua komponen tanda tangan elektronik. (2) Digunakan hanya oleh pemilik asli mereka; dan (3) Dikelola dan dilaksanakan untuk memastikan bahwa upaya penggunaan tanda tangan elektroni k individu oleh siapa pun selain pemilik aslinya memerlukan kolaborasi dua orang atau lebih.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	(a) Tanda tangan elektronik yang tidak didasarkan pada biometrik harus: (1) Menggunakan setidaknya dua komponen identifikasi yang berbeda seperti kode identifikasi dan kata sandi. (i) Ketika seorang individu mengeksekusi serangkaian penandatanganan selama satu periode akses sistem terkontrol yang berkelanjutan, penandatanganan pertama harus dijalankan menggunakan semua komponen tanda tangan elektronik; penandatanganan berikutnya harus dijalankan menggunakan setidaknya satu komponen tanda tangan elektronik yang hanya dapat dieksekusi oleh, dan dirancang untuk	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	digunakan hanya oleh, individu. (ii) Ketika seorang individu mengeksek usi satu atau lebih penandatanganan yang tidak dilakukan selama satu periode akses sistem terkontrol yang berkelanjutan, setiap penandatanganan harus dijalankan menggunakan semua komponen tanda tangan elektronik. (2) Digunakan hanya oleh pemilik asli mereka; dan (3) Dikelola dan dilaksanakan untuk memastikan bahwa upaya penggunaan tanda tangan elektroni k individu oleh siapa pun selain pemilik aslinya memerlukan kolaborasi dua orang atau lebih.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	(a) Tanda tangan elektronik yang tidak didasarkan pada biometrik harus: (1) Menggunakan setidaknya dua komponen identifikasi yang berbeda seperti kode identifikasi dan kata sandi. (i) Ketika seorang individu mengeksekusi serangkaian penandatanganan selama satu periode akses sistem terkontrol yang berkelanjutan, penandatanganan pertama harus dijalankan menggunakan semua komponen tanda tangan elektronik; penandatanganan berikutnya harus dijalankan menggunakan setidaknya satu komponen tanda tangan elektronik yang hanya dapat dieksekusi oleh, dan dirancang untuk	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	digunakan hanya oleh, individu. (ii) Ketika seorang individu mengeksek usi satu atau lebih penandatanganan yang tidak dilakukan selama satu periode akses sistem terkontrol yang berkelanjutan, setiap penandatanganan harus dijalankan menggunakan semua komponen tanda tangan elektronik. (2) Digunakan hanya oleh pemilik asli mereka; dan (3) Dikelola dan dilaksanakan untuk memastikan bahwa upaya penggunaan tanda tangan elektroni k individu oleh siapa pun selain pemilik aslinya memerlukan kolaborasi dua orang atau lebih.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	(a) Tanda tangan elektronik yang tidak didasarkan pada biometrik harus: (1) Menggunakan setidaknya dua komponen identifikasi yang berbeda seperti kode identifikasi dan kata sandi. (i) Ketika seorang individu mengeksekusi serangkaian penandatanganan selama satu periode akses sistem terkontrol yang berkelanjutan, penandatanganan pertama harus dijalankan menggunakan semua komponen tanda tangan elektronik; penandatanganan berikutnya harus dijalankan menggunakan setidaknya satu komponen tanda tangan elektronik yang hanya dapat dieksekusi oleh, dan dirancang untuk	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	digunakan hanya oleh, individu. (ii) Ketika seorang individu mengeksek usi satu atau lebih penandatanganan yang tidak dilakukan selama satu periode akses sistem terkontrol yang berkelanjutan, setiap penandatanganan harus dijalankan menggunakan semua komponen tanda tangan elektronik. (2) Digunakan hanya oleh pemilik asli mereka; dan (3) Dikelola dan dilaksanakan untuk memastikan bahwa upaya penggunaan tanda tangan elektroni k individu oleh siapa pun selain pemilik aslinya memerlukan kolaborasi dua orang atau lebih.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2	(a) Tanda tangan elektronik yang tidak didasarkan pada biometrik harus: (1) Menggunakan setidaknya dua komponen identifikasi yang berbeda seperti kode identifikasi dan kata sandi. (i) Ketika seorang individu mengeksekusi serangkaian penandatanganan selama satu periode akses sistem terkontrol yang berkelanjutan, penandatanganan pertama harus dijalankan menggunakan semua komponen tanda tangan elektronik; penandatanganan berikutnya harus dijalankan menggunakan setidaknya satu komponen tanda tangan elektronik yang hanya dapat dieksekusi oleh, dan dirancang untuk	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	digunakan hanya oleh, individu. (ii) Ketika seorang individu mengeksek usi satu atau lebih penandatanganan yang tidak dilakukan selama satu periode akses sistem terkontrol yang berkelanjutan, setiap penandatanganan harus dijalankan menggunakan semua komponen tanda tangan elektronik. (2) Digunakan hanya oleh pemilik asli mereka; dan (3) Dikelola dan dilaksanakan untuk memastikan bahwa upaya penggunaan tanda tangan elektroni k individu oleh siapa pun selain pemilik aslinya memerlukan kolaborasi dua orang atau lebih.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus, atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	codebuild-project-artifact-encryption	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk AWS CodeBuild artefak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	codebuild-project-s3-log-terenkripsi	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk AWS CodeBuild log Anda yang disimpan di Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	kinesis-stream-encrypted	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.3	Orang yang menggunakan sistem terbuka untuk membuat, memodifikasi, memelihara, atau mengirimkan catatan elektronik harus menggunakan prosedur dan kontrol yang dirancang untuk memastikan keaslian, integritas, dan, jika sesuai, kerahasiaan catatan elektronik dari titik pembuatannya hingga titik penerimaan mereka. Prosedur dan kontrol tersebut harus mencakup yang diidentifikasi dalam 11.10, yang sesuai, dan langkah-langkah tambahan seperti enkripsi dokumen dan penggunaan standar tanda tangan digital yang sesuai untuk memastikan, sebagaimana diperlukan dalam keadaan, mencatat keaslian, integritas, dan kerahasiaan.	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.300 (b)	Orang yang menggunakan tanda tangan elektronik berdasarkan penggunaan kode identifikasi yang dikombinasikan dengan kata sandi harus menggunakan kontrol untuk memastikan keamanan dan integritas mereka. Kontrol tersebut harus mencakup: (b) Memastikan bahwa kode identifikasi dan penerbitan kata sandi diperiksa, ditarik kembali, atau direvisi secara berkala (misalnya, untuk mencakup peristiwa seperti penuaan kata sandi).	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.300 (b)	Orang yang menggunakan tanda tangan elektronik berdasarkan penggunaan kode identifikasi yang dikombinasikan dengan kata sandi harus menggunakan kontrol untuk memastikan keamanan dan integritas mereka. Kontrol tersebut harus mencakup: (b) Memastikan bahwa kode identifikasi dan penerbitan kata sandi diperiksa, ditarik kembali, atau direvisi secara berkala (misalnya, untuk mencakup peristiwa seperti penuaan kata sandi).	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktifkan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediakan sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.300 (b)	Orang yang menggunakan tanda tangan elektronik berdasarkan penggunaan kode identifikasi yang dikombinasikan dengan kata sandi harus menggunakan kontrol untuk memastikan keamanan dan integritas mereka. Kontrol tersebut harus mencakup: (b) Memastikan bahwa kode identifikasi dan penerbitan kata sandi diperiksa, ditarik kembali, atau direvisi secara berkala (misalnya, untuk mencakup peristiwa seperti penuaan kata sandi).	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.300 (b)	Orang yang menggunakan tanda tangan elektronik berdasarkan penggunaan kode identifikasi yang dikombinasikan dengan kata sandi harus menggunakan kontrol untuk memastikan keamanan dan integritas mereka. Kontrol tersebut harus mencakup: (b) Memastikan bahwa kode identifikasi dan penerbitan kata sandi diperiksa, ditarik kembali, atau direvisi secara berkala (misalnya, untuk mencakup peristiwa seperti penuaan kata sandi).	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.300 (b)	Orang yang menggunakan tanda tangan elektronik berdasarkan penggunaan kode identifikasi yang dikombinasikan dengan kata sandi harus menggunakan kontrol untuk memastikan keamanan dan integritas mereka. Kontrol tersebut harus mencakup: (b) Memastikan bahwa kode identifikasi dan penerbitan kata sandi diperiksa, ditarik kembali, atau direvisi secara berkala (misalnya, untuk mencakup peristiwa seperti penuaan kata sandi).	secretsmanager-rotation-enabled-check	Aturan ini memastikan AWS rahasia Secrets Manager telah diaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.300 (b)	Orang yang menggunakan tanda tangan elektronik berdasarkan penggunaan kode identifikasi yang dikombinasikan dengan kata sandi harus menggunakan kontrol untuk memastikan keamanan dan integritas mereka. Kontrol tersebut harus mencakup: (b) Memastikan bahwa kode identifikasi dan penerbitan kata sandi diperiksa, ditarik kembali, atau direvisi secara berkala (misalnya, untuk mencakup peristiwa seperti penuaan kata sandi).	secretsmanager-scheduled-rotation-success-periksa	Aturan ini memastikan bahwa AWS rahasia Secrets Manager telah berhasil diputar sesuai dengan jadwal rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode di mana rahasia aktif, dan berpotensi mengurangi dampak bisnis jika dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.300 (d)	Orang yang menggunakan tanda tangan elektronik berdasarkan penggunaan kode identifikasi yang dikombinasikan dengan kata sandi harus menggunakan kontrol untuk memastikan keamanan dan integritas mereka. Pengendalian tersebut mencakup: (d) Penggunaan perlindungan transaksi untuk mencegah penggunaan kata sandi dan/atau kode identifikasi yang tidak sah, dan untuk mendeteksi dan melaporkan secara segera dan mendesak setiap upaya penggunaannya yang tidak sah ke unit keamanan sistem, dan, sebagaimana mestinya, kepada manajemen organisasi.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.300 (d)	Orang yang menggunakan tanda tangan elektronik berdasarkan penggunaan kode identifikasi yang dikombinasikan dengan kata sandi harus menggunakan kontrol untuk memastikan keamanan dan integritas mereka. Pengendalian tersebut mencakup: (d) Penggunaan perlindungan transaksi untuk mencegah penggunaan kata sandi dan/atau kode identifikasi yang tidak sah, dan untuk mendeteksi dan melaporkan secara segera dan mendesak setiap upaya penggunaannya yang tidak sah ke unit keamanan sistem, dan, sebagaimana mestinya, kepada manajemen organisasi.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.300 (d)	Orang yang menggunakan tanda tangan elektronik berdasarkan penggunaan kode identifikasi yang dikombinasikan dengan kata sandi harus menggunakan kontrol untuk memastikan keamanan dan integritas mereka. Pengendalian tersebut mencakup: (d) Penggunaan perlindungan transaksi untuk mencegah penggunaan kata sandi dan/atau kode identifikasi yang tidak sah, dan untuk mendeteksi dan melaporkan secara segera dan mendesak setiap upaya penggunaannya yang tidak sah ke unit keamanan sistem, dan, sebagaimana mestinya, kepada manajemen organisasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.300 (d)	Orang yang menggunakan tanda tangan elektronik berdasarkan penggunaan kode identifikasi yang dikombinasikan dengan kata sandi harus menggunakan kontrol untuk memastikan keamanan dan integritas mereka. Pengendalian tersebut mencakup: (d) Penggunaan perlindungan transaksi untuk mencegah penggunaan kata sandi dan/atau kode identifikasi yang tidak sah, dan untuk mendeteksi dan melaporkan secara segera dan mendesak setiap upaya penggunaannya yang tidak sah ke unit keamanan sistem, dan, sebagaimana mestinya, kepada manajemen organisasi.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk FDA Judul 21 CFR Bagian 11.

Praktik Terbaik Operasional untuk FedRAMP (Rendah)

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara Federal Risk and Authorization Management Program (FedRAMP) Low Baseline Controls dan aturan Config terkelola. AWS Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau beberapa kontrol FedRAMP. Kontrol FedRAMP dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	MANAJEMEN AKUN	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.
AC-2	MANAJEMEN AKUN	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual harus mencerminkan

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			kebijakan organisasi Anda
AC-2	MANAJEMEN AKUN	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	MANAJEMEN AKUN	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
AC-2	MANAJEMEN AKUN	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	MANAJEMEN AKUN	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	MANAJEMEN AKUN	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	MANAJEMEN AKUN	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	MANAJEMEN AKUN	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	MANAJEMEN AKUN	access-keys-rotated	Kredensi diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	MANAJEMEN AKUN	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
AC-2	MANAJEMEN AKUN	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	MANAJEMEN AKUN	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	MANAJEMEN AKUN	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	MANAJEMEN AKUN	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	MANAJEMEN AKUN	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	MANAJEMEN AKUN	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	MANAJEMEN AKUN	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	MANAJEMEN AKUN	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	MANAJEMEN AKUN	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	MANAJEMEN AKUN	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	MANAJEMEN AKUN	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	MANAJEMEN AKUN	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	MANAJEMEN AKUN	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	MANAJEMEN AKUN	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	MANAJEMEN AKUN	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	MANAJEMEN AKUN	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	PENEGAKAN AKSES	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	PENEGAKAN AKSES	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.
AC-3	PENEGAKAN AKSES	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	PENEGAKAN AKSES	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	PENEGAKAN AKSES	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	PENEGAKAN AKSES	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
AC-3	PENEGAKAN AKSES	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	PENEGAKAN AKSES	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-3	PENEGAKAN AKSES	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-3	PENEGAKAN AKSES	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	PENEGAKAN AKSES	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
AC-3	PENEGAKAN AKSES	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	PENEGAKAN AKSES	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	PENEGAKAN AKSES	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	PENEGAKAN AKSES	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	PENEGAKAN AKSES	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	PENEGAKAN AKSES	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	PENEGAKAN AKSES	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	PENEGAKAN AKSES	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	PENEGAKAN AKSES	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	PENEGAKAN AKSES	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	PENEGAKAN AKSES	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
AC-3	PENEGAKAN AKSES	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	PENEGAKAN AKSES	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	PENEGAKAN AKSES	s3- account-level-publ ic-access -blok-per iodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	PENEGAKAN AKSES	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
AC-3	PENEGAKAN AKSES	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	PENEGAKAN AKSES	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
AC-3	PENEGAKAN AKSES	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	PENEGAKAN AKSES	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
AC-17	AKSES JARAK JAUH	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17	AKSES JARAK JAUH	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17	AKSES JARAK JAUH	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17	AKSES JARAK JAUH	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17	AKSES JARAK JAUH	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
AC-17	AKSES JARAK JAUH	alb-http-to-https-pemeriksaan-pengalihan	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17	AKSES JARAK JAUH	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-17	AKSES JARAK JAUH	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-17	AKSES JARAK JAUH	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17	AKSES JARAK JAUH	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
AC-17	AKSES JARAK JAUH	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17	AKSES JARAK JAUH	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
AC-17	AKSES JARAK JAUH	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17	AKSES JARAK JAUH	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17	AKSES JARAK JAUH	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17	AKSES JARAK JAUH	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
AC-17	AKSES JARAK JAUH	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17	AKSES JARAK JAUH	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-17	AKSES JARAK JAUH	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17	AKSES JARAK JAUH	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17	AKSES JARAK JAUH	s3- account-level-publ ic-access -blok-per iodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17	AKSES JARAK JAUH	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
AC-17	AKSES JARAK JAUH	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17	AKSES JARAK JAUH	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
AC-17	AKSES JARAK JAUH	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17	AKSES JARAK JAUH	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
AC-17	AKSES JARAK JAUH	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17	AKSES JARAK JAUH	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17	AKSES JARAK JAUH	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2	ACARA AUDIT	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2	ACARA AUDIT	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2	ACARA AUDIT	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2	ACARA AUDIT	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
AU-2	ACARA AUDIT	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2	ACARA AUDIT	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
AU-2	ACARA AUDIT	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2	ACARA AUDIT	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
AU-2	ACARA AUDIT	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2	ACARA AUDIT	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2	ACARA AUDIT	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2	ACARA AUDIT	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
AU-3	ISI CATATAN AUDIT	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	ISI CATATAN AUDIT	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	ISI CATATAN AUDIT	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	ISI CATATAN AUDIT	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
AU-3	ISI CATATAN AUDIT	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	ISI CATATAN AUDIT	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
AU-3	ISI CATATAN AUDIT	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	ISI CATATAN AUDIT	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
AU-3	ISI CATATAN AUDIT	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	ISI CATATAN AUDIT	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDbEncrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	ISI CATATAN AUDIT	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	ISI CATATAN AUDIT	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
AU-6	TINJAUAN AUDIT, ANALISIS, DAN PELAPORAN	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6	TINJAUAN AUDIT, ANALISIS, DAN PELAPORAN	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6	TINJAUAN AUDIT, ANALISIS, DAN PELAPORAN	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6	TINJAUAN AUDIT, ANALISIS, DAN PELAPORAN	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6	TINJAUAN AUDIT, ANALISIS, DAN PELAPORAN	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
AU-6	TINJAUAN AUDIT, ANALISIS, DAN PELAPORAN	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6	TINJAUAN AUDIT, ANALISIS, DAN PELAPORAN	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
AU-6	TINJAUAN AUDIT, ANALISIS, DAN PELAPORAN	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6	TINJAUAN AUDIT, ANALISIS, DAN PELAPORAN	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6	TINJAUAN AUDIT, ANALISIS, DAN PELAPORAN	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6	TINJAUAN AUDIT, ANALISIS, DAN PELAPORAN	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6	TINJAUAN AUDIT, ANALISIS, DAN PELAPORAN	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6	TINJAUAN AUDIT, ANALISIS, DAN PELAPORAN	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6	TINJAUAN AUDIT, ANALISIS, DAN PELAPORAN	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6	TINJAUAN AUDIT, ANALISIS, DAN PELAPORAN	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6	TINJAUAN AUDIT, ANALISIS, DAN PELAPORAN	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-9	PERLINDUNGAN INFORMASI AUDIT	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.
AU-9	PERLINDUNGAN INFORMASI AUDIT	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrai l jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-9	PERLINDUNGAN INFORMASI AUDIT	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.
AU-9	PERLINDUNGAN INFORMASI AUDIT	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-9	PERLINDUNGAN INFORMASI AUDIT	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-11	RETENSI CATATAN AUDIT	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.
AU-12	PEMBUATAN AUDIT	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	PEMBUATAN AUDIT	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	PEMBUATAN AUDIT	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	PEMBUATAN AUDIT	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
AU-12	PEMBUATAN AUDIT	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	PEMBUATAN AUDIT	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
AU-12	PEMBUATAN AUDIT	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	PEMBUATAN AUDIT	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
AU-12	PEMBUATAN AUDIT	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	PEMBUATAN AUDIT	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	PEMBUATAN AUDIT	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	PEMBUATAN AUDIT	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
CA-7	PEMANTAUAN TERUS MENERUS	lambda-concurrency-check	Aturan ini memastikan bahwa batas tinggi dan rendah konkurensi fungsi Lambda ditetapkan. Ini dapat membantu dalam mendasarkan jumlah permintaan yang dilayani oleh fungsi Anda pada waktu tertentu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7	PEMANTAUAN TERUS MENERUS	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7	PEMANTAUAN TERUS MENERUS	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7	PEMANTAUAN TERUS MENERUS	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7	PEMANTAUAN TERUS MENERUS	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7	PEMANTAUAN TERUS MENERUS	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7	PEMANTAUAN TERUS MENERUS	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7	PEMANTAUAN TERUS MENERUS	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
CA-7	PEMANTAUAN TERUS MENERUS	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7	PEMANTAUAN TERUS MENERUS	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7	PEMANTAUAN TERUS MENERUS	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
CA-7	PEMANTAUAN TERUS MENERUS	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7	PEMANTAUAN TERUS MENERUS	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7	PEMANTAUAN TERUS MENERUS	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	KONFIGURASI DASAR	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	KONFIGURASI DASAR	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindungi nya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	KONFIGURASI DASAR	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
CM-2	KONFIGURASI DASAR	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	KONFIGURASI DASAR	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CM-2	KONFIGURASI DASAR	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	KONFIGURASI DASAR	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
CM-2	KONFIGURASI DASAR	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	KONFIGURASI DASAR	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	KONFIGURASI DASAR	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	KONFIGURASI DASAR	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	KONFIGURASI DASAR	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	KONFIGURASI DASAR	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
CM-2	KONFIGURASI DASAR	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	KONFIGURASI DASAR	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
CM-2	KONFIGURASI DASAR	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	KONFIGURASI DASAR	s3- account-level-publ ic-access -blok-per iodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	KONFIGURASI DASAR	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
CM-2	KONFIGURASI DASAR	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	KONFIGURASI DASAR	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	KONFIGURASI DASAR	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	KONFIGURASI DASAR	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	KONFIGURASI DASAR	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	KONFIGURASI DASAR	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	KONFIGURASI DASAR	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.
CM-2	KONFIGURASI DASAR	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	KONFIGURASI DASAR	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	KONFIGURASI DASAR	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	KONFIGURASI DASAR	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	KONFIGURASI DASAR	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	KONFIGURASI DASAR	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
CM-7	FUNGSIONALITAS PALING SEDIKIT	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-7	FUNGSIONALITAS PALING SEDIKIT	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-7	FUNGSIONALITAS PALING SEDIKIT	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-8	INVENTARIS KOMPONEN SISTEM INFORMASI	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-8	INVENTARIS KOMPONEN SISTEM INFORMASI	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-8	INVENTARIS KOMPONEN SISTEM INFORMASI	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-8	INVENTARIS KOMPONEN SISTEM INFORMASI	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	CADANGAN SISTEM INFORMASI	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	CADANGAN SISTEM INFORMASI	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	CADANGAN SISTEM INFORMASI	dynamodb-resources-protected-by-rencana cadangan	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	CADANGAN SISTEM INFORMASI	ebs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	CADANGAN SISTEM INFORMASI	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	CADANGAN SISTEM INFORMASI	efs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	CADANGAN SISTEM INFORMASI	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	CADANGAN SISTEM INFORMASI	rds-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Relational Database Service (Amazon RDS) Anda merupakan AWS bagian dari paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	CADANGAN SISTEM INFORMASI	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	CADANGAN SISTEM INFORMASI	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	CADANGAN SISTEM INFORMASI	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	CADANGAN SISTEM INFORMASI	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	CADANGAN SISTEM INFORMASI	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	CADANGAN SISTEM INFORMASI	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	PEMULIHAN DAN REKONSTITUSI SISTEM INFORMASI	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	PEMULIHAN DAN REKONSTITUSI SISTEM INFORMASI	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	PEMULIHAN DAN REKONSTITUSI SISTEM INFORMASI	dynamodb-resources-protected-by-rencana cadangan	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	PEMULIHAN DAN REKONSTITUSI SISTEM INFORMASI	ebs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	PEMULIHAN DAN REKONSTITUSI SISTEM INFORMASI	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	PEMULIHAN DAN REKONSTITUSI SISTEM INFORMASI	efs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	PEMULIHAN DAN REKONSTITUSI SISTEM INFORMASI	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	PEMULIHAN DAN REKONSTITUSI SISTEM INFORMASI	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	PEMULIHAN DAN REKONSTITUSI SISTEM INFORMASI	rds-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Relational Database Service (Amazon RDS) Anda merupakan AWS bagian dari paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	PEMULIHAN DAN REKONSTITUSI SISTEM INFORMASI	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	PEMULIHAN DAN REKONSTITUSI SISTEM INFORMASI	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	PEMULIHAN DAN REKONSTITUSI SISTEM INFORMASI	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	PEMULIHAN DAN REKONSTITUSI SISTEM INFORMASI	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	PEMULIHAN DAN REKONSTITUSI SISTEM INFORMASI	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	PEMULIHAN DAN REKONSTITUSI SISTEM INFORMASI	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	PEMULIHAN DAN REKONSTITUSI SISTEM INFORMASI	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	PEMULIHAN DAN REKONSTITUSI SISTEM INFORMASI	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	PEMULIHAN DAN REKONSTITUSI SISTEM INFORMASI	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	PEMULIHAN DAN REKONSTITUSI SISTEM INFORMASI	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	PEMULIHAN DAN REKONSTITUSI SISTEM INFORMASI	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2	IDENTIFIKASI DAN OTENTIKASI (PENGGUNA ORGANISASI)	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2	IDENTIFIKASI DAN OTENTIKASI (PENGGUNA ORGANISASI)	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2	IDENTIFIKASI DAN OTENTIKASI (PENGGUNA ORGANISASI)	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2	IDENTIFIKASI DAN OTENTIKASI (PENGGUNA ORGANISASI)	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2	IDENTIFIKASI DAN OTENTIKASI (PENGGUNA ORGANISASI)	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2	IDENTIFIKASI DAN OTENTIKASI (PENGGUNA ORGANISASI)	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-5	MANAJEMEN AUTENTIKATOR	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild . Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-5	MANAJEMEN AUTENTIKATOR	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-4	PENANGANAN INSIDEN	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-4	PENANGANAN INSIDEN	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-4	PENANGANAN INSIDEN	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-4	PENANGANAN INSIDEN	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-4	PENANGANAN INSIDEN	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-6	PELAPORAN INSIDEN	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-6	PELAPORAN INSIDEN	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-6	PELAPORAN INSIDEN	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-7	BANTUAN RESPON INSIDEN	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-7	BANTUAN RESPON INSIDEN	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-7	BANTUAN RESPON INSIDEN	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RA-5	PEMINDAIAN KERENTANAN	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RA-5	PEMINDAIAN KERENTANAN	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RA-5	PEMINDAIAN KERENTANAN	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-3	SIKLUS HIDUP PENGEMBANGAN SISTEM	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild . Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-3	SIKLUS HIDUP PENGEMBANGAN SISTEM	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredenal masuk dalam lingkungan proyek Codebuild . AWS Gunakan OAuth alih-alih token akses pribadi atau kredensi masuk untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-3	SIKLUS HIDUP PENGEMBANGAN SISTEM	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	PENOLAKAN PERLINDUNGAN LAYANAN	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	PENOLAKAN PERLINDUNGAN LAYANAN	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	PENOLAKAN PERLINDUNGAN LAYANAN	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	PENOLAKAN PERLINDUNGAN LAYANAN	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	PENOLAKAN PERLINDUNGAN LAYANAN	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	PENOLAKAN PERLINDUNGAN LAYANAN	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	PENOLAKAN PERLINDUNGAN LAYANAN	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	PENOLAKAN PERLINDUNGAN LAYANAN	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	PENOLAKAN PERLINDUNGAN LAYANAN	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	PENOLAKAN PERLINDUNGAN LAYANAN	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	PENOLAKAN PERLINDUNGAN LAYANAN	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	PENOLAKAN PERLINDUNGAN LAYANAN	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	PENOLAKAN PERLINDUNGAN LAYANAN	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	PERLINDUNGAN BATAS	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	PERLINDUNGAN BATAS	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
SC-7	PERLINDUNGAN BATAS	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	PERLINDUNGAN BATAS	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	PERLINDUNGAN BATAS	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
SC-7	PERLINDUNGAN BATAS	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	PERLINDUNGAN BATAS	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	PERLINDUNGAN BATAS	alb-http-to-https-pemeriksaan-pengalihan	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	PERLINDUNGAN BATAS	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	PERLINDUNGAN BATAS	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	PERLINDUNGAN BATAS	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
SC-7	PERLINDUNGAN BATAS	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	PERLINDUNGAN BATAS	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
SC-7	PERLINDUNGAN BATAS	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	PERLINDUNGAN BATAS	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	PERLINDUNGAN BATAS	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
SC-7	PERLINDUNGAN BATAS	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	PERLINDUNGAN BATAS	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-7	PERLINDUNGAN BATAS	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	PERLINDUNGAN BATAS	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	PERLINDUNGAN BATAS	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	PERLINDUNGAN BATAS	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	PERLINDUNGAN BATAS	waf-regional-webacl-not-kosong	Web ACL yang dilampirkan ke AWS WAF dapat berisi kumpulan aturan dan kelompok aturan untuk memeriksa dan mengontrol permintaan web. Jika ACL Web kosong, lalu lintas web lewat tanpa terdeteksi atau ditindaklanjuti oleh WAF.
SC-12	PEMBENTUKAN DAN MANAJEMEN KUNCI KRIPTOGRAFI	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-12	PEMBENTUKAN DAN MANAJEMEN KUNCI KRIPTOGRAFI	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-12	PEMBENTUKAN DAN MANAJEMEN KUNCI KRIPTOGRAFI	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13	PERLINDUNGAN KRIPTOGRAFI	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.
SC-13	PERLINDUNGAN KRIPTOGRAFI	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13	PERLINDUNGAN KRIPTOGRAFI	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-13	PERLINDUNGAN KRIPTOGRAFI	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13	PERLINDUNGAN KRIPTOGRAFI	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13	PERLINDUNGAN KRIPTOGRAFI	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2	REMEDIASI CACAT	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2	REMEDIASI CACAT	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2	REMEDIASI CACAT	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
SI-2	REMEDIASI CACAT	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-3	REMEDIASI CACAT	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild . Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-3	REMEDIASI CACAT	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredenal masuk dalam lingkungan proyek Codebuild . AWS Gunakan OAuth alih-alih token akses pribadi atau kredensi masuk untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.
SI-3	REMEDIASI CACAT	ecs-task-definition-memory-batas-keras	Membatasi memori maksimum yang tersedia untuk penampung Amazon Elastic Container Service (ECS) memastikan bahwa penggunaan sumber daya Anda tidak dapat disalahgunakan jika terjadi akses berbahaya ke kontainer Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4	PEMANTAUAN SISTEM INFORMASI	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4	PEMANTAUAN SISTEM INFORMASI	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindungi nya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4	PEMANTAUAN SISTEM INFORMASI	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4	PEMANTAUAN SISTEM INFORMASI	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4	PEMANTAUAN SISTEM INFORMASI	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4	PEMANTAUAN SISTEM INFORMASI	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
SI-4	PEMANTAUAN SISTEM INFORMASI	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4	PEMANTAUAN SISTEM INFORMASI	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
SI-4	PEMANTAUAN SISTEM INFORMASI	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4	PEMANTAUAN SISTEM INFORMASI	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4	PEMANTAUAN SISTEM INFORMASI	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.
SI-4	PEMANTAUAN SISTEM INFORMASI	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4	PEMANTAUAN SISTEM INFORMASI	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-5	PERINGATAN KEAMANAN, SARAN, DAN ARAHAN	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-5	PERINGATAN KEAMANAN, SARAN, DAN ARAHAN	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-5	PERINGATAN KEAMANAN, SARAN, DAN ARAHAN	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-5	PERINGATAN KEAMANAN, SARAN, DAN ARAHAN	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	PENANGANAN DAN RETENSI INFORMASI	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	PENANGANAN DAN RETENSI INFORMASI	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	PENANGANAN DAN RETENSI INFORMASI	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	PENANGANAN DAN RETENSI INFORMASI	dynamodb-resources-protected-by-rencana cadangan	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	PENANGANAN DAN RETENSI INFORMASI	ebs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	PENANGANAN DAN RETENSI INFORMASI	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	PENANGANAN DAN RETENSI INFORMASI	efs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	PENANGANAN DAN RETENSI INFORMASI	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	PENANGANAN DAN RETENSI INFORMASI	rds-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Relational Database Service (Amazon RDS) Anda merupakan AWS bagian dari paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	PENANGANAN DAN RETENSI INFORMASI	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	PENANGANAN DAN RETENSI INFORMASI	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	PENANGANAN DAN RETENSI INFORMASI	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	PENANGANAN DAN RETENSI INFORMASI	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	PENANGANAN DAN RETENSI INFORMASI	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-16	PERLINDUNGAN MEMORI	ecs-task-definition-memory-batas-keras	Membatasi memori maksimum yang tersedia untuk penampung Amazon Elastic Container Service (ECS) memastikan bahwa penggunaan sumber daya Anda tidak dapat disalahgu nakan jika terjadi akses berbahaya ke kontainer Anda.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk FedRAMP (Rendah).

Praktik Terbaik Operasional untuk FedRAMP (Sedang)

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara Federal Risk and Authorization Management Program (FedRAMP) dan aturan Config terkelola. AWS Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau beberapa kontrol FedRAMP. Kontrol FedRAMP dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

Paket Kesesuaian ini divalidasi oleh AWS Security Assurance Services LLC (AWS SAS), yang merupakan tim dari Payment Card Industry Qualified Security Assesors (QSAs), HITRUST Certified

Common Security Framework Practitioners (CCSFPs), dan profesional kepatuhan yang disertifikasi untuk memberikan panduan dan penilaian untuk berbagai kerangka kerja industri. AWS Profesional SAS merancang Paket Kesesuaian ini untuk memungkinkan pelanggan menyelaraskan dengan subset kontrol FedRAMP.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (3)	Sistem informasi secara otomatis menonaktifkan akun yang tidak aktif setelah 90 hari untuk pengguna.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (3)	Sistem informasi secara otomatis menonaktifkan akun yang tidak aktif setelah 90 hari untuk pengguna.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikasi, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisasi].	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikasi, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisasi].	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikasi, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisasi].	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikasi, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisasi].	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikasi, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisasi].	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikasi, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisasi].	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikasi, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisasi].	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikasi, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisasi].	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikasi, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisasi].	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikasi, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisasi].	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDbEncrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikasi, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisasi].	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (7)	Organisasi: (a) Menetapkan dan mengelola pengguna istimewa sesuai dengan skema akses berbasis peran yang mengatur akses sistem informasi yang diizinkan dan hak istimewa ke dalam peran; (b) Memantau tugas peran istimewa; dan (c) Mengambil [Penugasan: tindakan yang ditentukan organisasi] ketika tugas peran istimewa tidak lagi sesuai. Panduan Tambahan: Peran istimewa adalah peran yang ditentukan organisas i yang diberikan kepada individu yang memungkin kan individu tersebut melakukan fungsi tertentu yang relevan dengan keamanan yang tidak diizinkan oleh pengguna biasa. Peran istimewa ini termasuk, misalnya, manajemen kunci,	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	manajemen akun, administrasi jaringan dan sistem, administrasi basis data, dan administrasi web.		harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (7)	Organisasi: (a) Menetapkan dan mengelola pengguna istimewa sesuai dengan skema akses berbasis peran yang mengatur akses sistem informasi yang diizinkan dan hak istimewa ke dalam peran; (b) Memantau tugas peran istimewa; dan (c) Mengambil [Penugasan: tindakan yang ditentukan organisasi] ketika tugas peran istimewa tidak lagi sesuai. Panduan Tambahan: Peran istimewa adalah peran yang ditentukan organisasi yang diberikan kepada individu yang memungkinkan individu tersebut melakukan fungsi tertentu yang relevan dengan keamanan yang tidak diizinkan oleh pengguna biasa. Peran istimewa ini termasuk, misalnya, manajemen kunci,	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	manajemen akun, administrasi jaringan dan sistem, administrasi basis data, dan administrasi web.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (7)	Organisasi: (a) Menetapkan dan mengelola pengguna istimewa sesuai dengan skema akses berbasis peran yang mengatur akses sistem informasi yang diizinkan dan hak istimewa ke dalam peran; (b) Memantau tugas peran istimewa; dan (c) Mengambil [Penugasan: tindakan yang ditentukan organisasi] ketika tugas peran istimewa tidak lagi sesuai. Panduan Tambahan: Peran istimewa adalah peran yang ditentukan organisasi yang diberikan kepada individu yang memungkinkan individu tersebut melakukan fungsi tertentu yang relevan dengan keamanan yang tidak diizinkan oleh pengguna biasa. Peran istimewa ini termasuk, misalnya, manajemen kunci,	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi, pengembalian, dan pendelegasian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	manajemen akun, administrasi jaringan dan sistem, administrasi basis data, dan administrasi web.		harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (7)	Organisasi: (a) Menetapkan dan mengelola pengguna istimewa sesuai dengan skema akses berbasis peran yang mengatur akses sistem informasi yang diizinkan dan hak istimewa ke dalam peran; (b) Memantau tugas peran istimewa; dan (c) Mengambil [Penugasan: tindakan yang ditentukan organisasi] ketika tugas peran istimewa tidak lagi sesuai. Panduan Tambahan: Peran istimewa adalah peran yang ditentukan organisasi yang diberikan kepada individu yang memungkinkan individu tersebut melakukan fungsi tertentu yang relevan dengan keamanan yang tidak diizinkan oleh pengguna biasa. Peran istimewa ini termasuk, misalnya, manajemen kunci,	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	manajemen akun, administrasi jaringan dan sistem, administrasi basis data, dan administrasi web.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (7)	Organisasi: (a) Menetapkan dan mengelola pengguna istimewa sesuai dengan skema akses berbasis peran yang mengatur akses sistem informasi yang diizinkan dan hak istimewa ke dalam peran; (b) Memantau tugas peran istimewa; dan (c) Mengambil [Penugasan: tindakan yang ditentukan organisasi] ketika tugas peran istimewa tidak lagi sesuai. Panduan Tambahan: Peran istimewa adalah peran yang ditentukan organisasi yang diberikan kepada individu yang memungkinkan individu tersebut melakukan fungsi tertentu yang relevan dengan keamanan yang tidak diizinkan oleh pengguna biasa. Peran istimewa ini termasuk, misalnya, manajemen kunci,	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	manajemen akun, administrasi jaringan dan sistem, administrasi basis data, dan administrasi web.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (7)	Organisasi: (a) Menetapkan dan mengelola pengguna istimewa sesuai dengan skema akses berbasis peran yang mengatur akses sistem informasi yang diizinkan dan hak istimewa ke dalam peran; (b) Memantau tugas peran istimewa; dan (c) Mengambil [Penugasan: tindakan yang ditentukan organisasi] ketika tugas peran istimewa tidak lagi sesuai. Panduan Tambahan: Peran istimewa adalah peran yang ditentukan organisasi yang diberikan kepada individu yang memungkinkan individu tersebut melakukan fungsi tertentu yang relevan dengan keamanan yang tidak diizinkan oleh pengguna biasa. Peran istimewa ini termasuk, misalnya, manajemen kunci,	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	manajemen akun, administrasi jaringan dan sistem, administrasi basis data, dan administrasi web.		
AC-2 (12) (a)	Organisasi: a. Memantau akun sistem informasi untuk [Penugasan: penggunaan atipikal yang ditentukan organisasi].	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (12) (a)	Organisasi: a. Memantau akun sistem informasi untuk [Penugasan: penggunaan atipikal yang ditentukan organisasi].	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (f)	Organisasi: f. Membuat, mengaktif kan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisas i].	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
AC-2 (f)	Organisasi: f. Membuat, mengaktif kan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisas i].	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (f)	Organisasi: f. Membuat, mengaktifkan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisasi].	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (f)	Organisasi: f. Membuat, mengaktifkan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisasi].	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (f)	Organisasi: f. Membuat, mengaktif kan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisas i].	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastika n kunci akses IAM diputar sebagaima na ditentukan oleh kebijakan organisas i. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurang i dampak bisnis jika kunci dikompromikan. Aturan ini memerluka n nilai rotasi kunci akses (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (f)	Organisasi: f. Membuat, mengaktif kan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisas i].	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifik asi berdasark an kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkin kan Anda untuk mengatur secara opsional RequireUp percaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (f)	Organisasi: f. Membuat, mengaktif kan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisas i].	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (f)	Organisasi: f. Membuat, mengaktifkan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisasi].	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (f)	Organisasi: f. Membuat, mengaktif kan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisas i].	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastika n otentikasi multi-fak tor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (f)	Organisasi: f. Membuat, mengaktif kan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisas i].	iam-user-no-policies-periksa	Aturan ini memastika n kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapka n hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (f)	Organisasi: f. Membuat, mengaktifkan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisasi].	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (f)	Organisasi: f. Membuat, mengaktif kan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisas i].	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (f)	Organisasi: f. Membuat, mengaktif kan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisas i].	root-account-hardw are-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindun gan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (f)	Organisasi: f. Membuat, mengaktif kan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisas i].	root-account-mfa-e nabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindun gan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	api-gw-execution-l ogging-diaktifkan	Pencatatan API Gateway menampilk an tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	ec2- instance-profile-a ttached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirk an profil instans ke instans Anda dapat membantu pengelola an hak istimewa dan izin paling sedikit.
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-policy-no-stat ements-with-full-a ccess	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastika n otentikasi multi-fak tor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-user-unused-cr edentials-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCreden tialUsage Usia (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastika n kunci akses IAM diputar sebagaima na ditentukan oleh kebijakan organisas i. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurang i dampak bisnis jika kunci dikompromikan. Aturan ini memerluka n nilai rotasi kunci akses (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifik asi berdasark an kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkin kan Anda untuk mengatur secara opsional RequireUp percaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-user-group-mem bership-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastika n pengguna adalah anggota setidaknya satu grup. Mengizink an pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-user-no-policies-periksa	Aturan ini memastika n kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapka n hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	root-account-mfa-e nabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindun gan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	acm-certificate-ex piration-check	Pastikan integritas jaringan dilindungi dengan memastika n sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExp iration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSear ch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerluka n gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	lambda-function-pu blic-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotens i menyebabkan degradasi ketersedi aan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	sagemaker-notebook -no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/ 0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-5c	Organisasi: c. Mendefinisikan otorisasi akses sistem informasi untuk mendukung pemisahan tugas.	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-5c	Organisasi: c. Mendefinisikan otorisasi akses sistem informasi untuk mendukung pemisahan tugas.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-5c	Organisasi: c. Mendefinisikan otorisasi akses sistem informasi untuk mendukung pemisahan tugas.	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
AC-5c	Organisasi: c. Mendefinisikan otorisasi akses sistem informasi untuk mendukung pemisahan tugas.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-5c	Organisasi: c. Mendefinisikan otorisasi akses sistem informasi untuk mendukung pemisahan tugas.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-5c	Organisasi: c. Mendefinisikan otorisasi akses sistem informasi untuk mendukung pemisahan tugas.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
AC-5c	Organisasi: c. Mendefinisikan otorisasi akses sistem informasi untuk mendukung pemisahan tugas.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-5c	Organisasi: c. Mendefinisikan otorisasi akses sistem informasi untuk mendukung pemisahan tugas.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-5c	Organisasi: c. Mendefinisikan otorisasi akses sistem informasi untuk mendukung pemisahan tugas.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-5c	Organisasi: c. Mendefinisikan otorisasi akses sistem informasi untuk mendukung pemisahan tugas.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-5c	Organisasi: c. Mendefinisikan otorisasi akses sistem informasi untuk mendukung pemisahan tugas.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-5c	Organisasi: c. Mendefinisikan otorisasi akses sistem informasi untuk mendukung pemisahan tugas.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.
AC-6 (10)	Sistem informasi mencegah pengguna yang tidak memiliki hak istimewa untuk menjalankan fungsi istimewa untuk menyertakan menonaktifkan, menghindari, atau mengubah pengamanan keamanan/penanggulangan yang diterapkan.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (10)	Sistem informasi mencegah pengguna yang tidak memiliki hak istimewa untuk menjalankan fungsi istimewa untuk menyertakan menonaktifkan, menghindari, atau mengubah pengamanan keamanan/penanggulangan yang diterapkan.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (10)	Sistem informasi mencegah pengguna yang tidak memiliki hak istimewa untuk menjalankan fungsi istimewa untuk menyertakan menonaktifkan, menghindari, atau mengubah pengamanan keamanan/penanggulangan yang diterapkan.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild . Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (2)	Sistem informasi menerapkan mekanisme kriptografi untuk melindungi kerahasiaan dan integritas sesi akses jarak jauh.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
AC-17 (2)	Sistem informasi menerapkan mekanisme kriptografi untuk melindungi kerahasiaan dan integritas sesi akses jarak jauh.	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (2)	Sistem informasi menerapkan mekanisme kriptografi untuk melindungi kerahasiaan dan integritas sesi akses jarak jauh.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
AC-17 (2)	Sistem informasi menerapkan mekanisme kriptografi untuk melindungi kerahasiaan dan integritas sesi akses jarak jauh.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (2)	Sistem informasi menerapkan mekanisme kriptografi untuk melindungi kerahasiaan dan integritas sesi akses jarak jauh.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa berikut: Kejadian login akun yang berhasil dan tidak berhasil, peristiwa manajemen akun, akses objek, perubahan kebijakan, fungsi hak istimewa, pelacakan proses, dan peristiwa sistem. Untuk aplikasi Web: semua aktivitas administrator, pemeriksaan otentikasi, pemeriksaan otorisasi, penghapusan data, akses data, perubahan data, dan perubahan izin. d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [subset yang ditentukan organisasi dari peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a untuk diaudit terus	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	menerus untuk setiap peristiwa yang diidentifikasi].		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa berikut: Kejadian login akun yang berhasil dan tidak berhasil, peristiwa manajemen akun, akses objek, perubahan kebijakan , fungsi hak istimewa, pelacakan proses, dan peristiwa sistem. Untuk aplikasi Web: semua aktivitas administr ator, pemeriksa an otentikasi, pemeriksaan otorisasi , penghapusan data, akses data, perubahan data, dan perubahan izin. d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [subset yang ditentuka n organisasi dari peristiwa yang dapat diaudit yang didefinis ikan dalam AU-2 a untuk diaudit terus	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	menerus untuk setiap peristiwa yang diidentifikasi].		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa berikut: Kejadian login akun yang berhasil dan tidak berhasil, peristiwa manajemen akun, akses objek, perubahan kebijakan , fungsi hak istimewa, pelacakan proses, dan peristiwa sistem. Untuk aplikasi Web: semua aktivitas administr ator, pemeriksa an otentikasi, pemeriksaan otorisasi , penghapusan data, akses data, perubahan data, dan perubahan izin. d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [subset yang ditentuka n organisasi dari peristiwa yang dapat diaudit yang didefinis ikan dalam AU-2 a untuk diaudit terus	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	menerus untuk setiap peristiwa yang diidentifikasi].		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa berikut: Kejadian login akun yang berhasil dan tidak berhasil, peristiwa manajemen akun, akses objek, perubahan kebijakan, fungsi hak istimewa, pelacakan proses, dan peristiwa sistem. Untuk aplikasi Web: semua aktivitas administrator, pemeriksaan otentikasi, pemeriksaan otorisasi, penghapusan data, akses data, perubahan data, dan perubahan izin. d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [subset yang ditentukan organisasi dari peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a untuk diaudit terus	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	menerus untuk setiap peristiwa yang diidentifikasi].		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa berikut: Kejadian login akun yang berhasil dan tidak berhasil, peristiwa manajemen akun, akses objek, perubahan kebijakan , fungsi hak istimewa, pelacakan proses, dan peristiwa sistem. Untuk aplikasi Web: semua aktivitas administr ator, pemeriksa an otentikasi, pemeriksaan otorisasi , penghapusan data, akses data, perubahan data, dan perubahan izin. d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [subset yang ditentuka n organisasi dari peristiwa yang dapat diaudit yang didefinis ikan dalam AU-2 a untuk diaudit terus	api-gw-execution-l ogging-diaktifkan	Pencatatan API Gateway menampilk an tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	menerus untuk setiap peristiwa yang diidentifikasi].		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa berikut: Kejadian login akun yang berhasil dan tidak berhasil, peristiwa manajemen akun, akses objek, perubahan kebijakan , fungsi hak istimewa, pelacakan proses, dan peristiwa sistem. Untuk aplikasi Web: semua aktivitas administr ator, pemeriksa an otentikasi, pemeriksaan otorisasi , penghapusan data, akses data, perubahan data, dan perubahan izin. d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [subset yang ditentuka n organisasi dari peristiwa yang dapat diaudit yang didefinis ikan dalam AU-2 a untuk diaudit terus	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	menerus untuk setiap peristiwa yang diidentifikasi].		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa berikut: Kejadian login akun yang berhasil dan tidak berhasil, peristiwa manajemen akun, akses objek, perubahan kebijakan , fungsi hak istimewa, pelacakan proses, dan peristiwa sistem. Untuk aplikasi Web: semua aktivitas administr ator, pemeriksa an otentikasi, pemeriksaan otorisasi , penghapusan data, akses data, perubahan data, dan perubahan izin. d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [subset yang ditentuka n organisasi dari peristiwa yang dapat diaudit yang didefinis ikan dalam AU-2 a untuk diaudit terus	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	menerus untuk setiap peristiwa yang diidentifikasi].		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa berikut: Kejadian login akun yang berhasil dan tidak berhasil, peristiwa manajemen akun, akses objek, perubahan kebijakan , fungsi hak istimewa, pelacakan proses, dan peristiwa sistem. Untuk aplikasi Web: semua aktivitas administr ator, pemeriksa an otentikasi, pemeriksaan otorisasi , penghapusan data, akses data, perubahan data, dan perubahan izin. d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [subset yang ditentuka n organisasi dari peristiwa yang dapat diaudit yang didefinis ikan dalam AU-2 a untuk diaudit terus	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteks i aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	menerus untuk setiap peristiwa yang diidentifikasi].		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa berikut: Kejadian login akun yang berhasil dan tidak berhasil, peristiwa manajemen akun, akses objek, perubahan kebijakan, fungsi hak istimewa, pelacakan proses, dan peristiwa sistem. Untuk aplikasi Web: semua aktivitas administrator, pemeriksaan otentikasi, pemeriksaan otorisasi, penghapusan data, akses data, perubahan data, dan perubahan izin. d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [subset yang ditentukan organisasi dari peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a untuk diaudit terus	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	menerus untuk setiap peristiwa yang diidentifikasi].		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa berikut: Kejadian login akun yang berhasil dan tidak berhasil, peristiwa manajemen akun, akses objek, perubahan kebijakan, fungsi hak istimewa, pelacakan proses, dan peristiwa sistem. Untuk aplikasi Web: semua aktivitas administrator, pemeriksaan otentikasi, pemeriksaan otorisasi, penghapusan data, akses data, perubahan data, dan perubahan izin. d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [subset yang ditentukan organisasi dari peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a untuk diaudit terus	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	menerus untuk setiap peristiwa yang diidentifikasi].		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa berikut: Kejadian login akun yang berhasil dan tidak berhasil, peristiwa manajemen akun, akses objek, perubahan kebijakan , fungsi hak istimewa, pelacakan proses, dan peristiwa sistem. Untuk aplikasi Web: semua aktivitas administr ator, pemeriksa an otentikasi, pemeriksaan otorisasi , penghapusan data, akses data, perubahan data, dan perubahan izin. d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [subset yang ditentuka n organisasi dari peristiwa yang dapat diaudit yang didefinis ikan dalam AU-2 a untuk diaudit terus	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediak an metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinc i untuk permintaa n yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	menerus untuk setiap peristiwa yang diidentifikasi].		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa berikut: Kejadian login akun yang berhasil dan tidak berhasil, peristiwa manajemen akun, akses objek, perubahan kebijakan , fungsi hak istimewa, pelacakan proses, dan peristiwa sistem. Untuk aplikasi Web: semua aktivitas administr ator, pemeriksa an otentikasi, pemeriksaan otorisasi , penghapusan data, akses data, perubahan data, dan perubahan izin. d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [subset yang ditentuka n organisasi dari peristiwa yang dapat diaudit yang didefinis ikan dalam AU-2 a untuk diaudit terus	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	menerus untuk setiap peristiwa yang diidentifikasi].		
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	codebuild-project-logging-enabled	Pastikan pencatata n AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatc h atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	cw-loggroup-retent ion-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonst ruksi dan mengident ifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisas i menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisas i untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisas i menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	wafv2-logging-diak tifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatata n AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
AU-7 (1)	Sistem informasi menyediakan kemampuan untuk memproses catatan audit untuk peristiwa yang menarik berdasarkan [Penugasan: bidang audit yang ditentuka n organisasi dalam catatan audit].	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-7 (1)	Sistem informasi menyediakan kemampuan untuk memproses catatan audit untuk peristiwa yang menarik berdasarkan [Penugasan: bidang audit yang ditentuka n organisasi dalam catatan audit].	cloudwatch-alarm-a ction-check	Amazon CloudWatc h mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasark an pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActi onRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-9 (2)	Sistem informasi mencadangkan catatan audit setidaknya setiap minggu ke sistem atau komponen sistem yang berbeda secara fisik dari sistem atau komponen yang diaudit.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-9 (2)	Sistem informasi mencadangkan catatan audit setidaknya setiap minggu ke sistem atau komponen sistem yang berbeda secara fisik dari sistem atau komponen yang diaudit.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.
AU-9	Sistem informasi melindungi informasi audit dan alat audit dari akses, modifikas i, dan penghapusan yang tidak sah.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrai l jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-9	Sistem informasi melindungi informasi audit dan alat audit dari akses, modifikasi, dan penghapusan yang tidak sah.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus, atau memalsukan CloudTrail file log tanpa deteksi.
AU-9	Sistem informasi melindungi informasi audit dan alat audit dari akses, modifikasi, dan penghapusan yang tidak sah.	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-11	Organisasi menyimpan catatan audit setidakny a selama 90 hari untuk memberika n dukungan untuk after-the-fact investigasi insiden keamanan dan untuk memenuhi persyarat an penyimpanan informasi peraturan dan organisasi.	cw-loggroup-retent ion-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonst ruksi dan mengident ifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di semua sistem informasi dan komponen jaringan di mana kemampuan audit disebarkan/tersedia c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di semua sistem informasi dan komponen jaringan di mana kemampuan audit disebarkan/tersedia c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di semua sistem informasi dan komponen jaringan di mana kemampuan audit disebarkan/tersedia c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di semua sistem informasi dan komponen jaringan di mana kemampuan audit disebarkan/tersedia c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di semua sistem informasi dan komponen jaringan di mana kemampuan audit disebarkan/tersedia c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di semua sistem informasi dan komponen jaringan di mana kemampuan audit disebarkan/tersedia c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di semua sistem informasi dan komponen jaringan di mana kemampuan audit disebarkan/tersedia c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di semua sistem informasi dan komponen jaringan di mana kemampuan audit disebarkan/tersedia c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di semua sistem informasi dan komponen jaringan di mana kemampuan audit disebarkan/tersedia c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di semua sistem informasi dan komponen jaringan di mana kemampuan audit disebarkan/tersedia c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di semua sistem informasi dan komponen jaringan di mana kemampuan audit disebarkan/tersedia c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di semua sistem informasi dan komponen jaringan di mana kemampuan audit disebarkan/tersedia c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantauan berkelanjutan dan menerapkan program pemantauan berkelanjutan yang meliputi: a. Pembentukan [Penugasan: metrik yang ditentukan organisasi] untuk dipantau; b. Pembentukan [Penugasan: frekuensi yang ditentukan organisasi] untuk pemantauan dan [Penugasan: frekuensi yang ditentukan organisasi] untuk penilaian yang mendukung pemantauan tersebut	lambda-concurrency-check	Aturan ini memastikan bahwa batas tinggi dan rendah konkurensi fungsi Lambda ditetapkan. Ini dapat membantu dalam mendasarkan jumlah permintaan yang dilayani oleh fungsi Anda pada waktu tertentu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantaua n berkelanjutan dan menerapkan program pemantauan berkelanj utan yang meliputi: a. Pembentuk an [Penugasa n: metrik yang ditentukan organisas i] untuk dipantau; b. Pembentuk an [Penugasan: frekuensi yang ditentukan organisas i] untuk pemantaua n dan [Penugasa n: frekuensi yang ditentukan organisas i] untuk penilaian yang mendukung pemantauan tersebut	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantaua n berkelanjutan dan menerapkan program pemantauan berkelanj utan yang meliputi: a. Pembentuk an [Penugasa n: metrik yang ditentukan organisas i] untuk dipantau; b. Pembentuk an [Penugasan: frekuensi yang ditentukan organisas i] untuk pemantaua n dan [Penugasa n: frekuensi yang ditentukan organisas i] untuk penilaian yang mendukung pemantauan tersebut	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantauan berkelanjutan dan menerapkan program pemantauan berkelanjutan yang meliputi: a. Pembentukan [Penugasan: metrik yang ditentukan organisasi] untuk dipantau; b. Pembentukan [Penugasan: frekuensi yang ditentukan organisasi] untuk pemantauan dan [Penugasan: frekuensi yang ditentukan organisasi] untuk penilaian yang mendukung pemantauan tersebut	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantaua n berkelanjutan dan menerapkan program pemantauan berkelanj utan yang meliputi: a. Pembentuk an [Penugasa n: metrik yang ditentukan organisas i] untuk dipantau; b. Pembentuk an [Penugasan: frekuensi yang ditentukan organisas i] untuk pemantaua n dan [Penugasa n: frekuensi yang ditentukan organisas i] untuk penilaian yang mendukung pemantauan tersebut	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantauan berkelanjutan dan menerapkan program pemantauan berkelanjutan yang meliputi: a. Pembentukan [Penugasan: metrik yang ditentukan organisasi] untuk dipantau; b. Pembentukan [Penugasan: frekuensi yang ditentukan organisasi] untuk pemantauan dan [Penugasan: frekuensi yang ditentukan organisasi] untuk penilaian yang mendukung pemantauan tersebut	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantauan berkelanjutan dan menerapkan program pemantauan berkelanjutan yang meliputi: a. Pembentukan [Penugasan: metrik yang ditentukan organisasi] untuk dipantau; b. Pembentukan [Penugasan: frekuensi yang ditentukan organisasi] untuk pemantauan dan [Penugasan: frekuensi yang ditentukan organisasi] untuk penilaian yang mendukung pemantauan tersebut	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantaua n berkelanjutan dan menerapkan program pemantauan berkelanj utan yang meliputi: a. Pembentuk an [Penugasa n: metrik yang ditentukan organisas i] untuk dipantau; b. Pembentuk an [Penugasan: frekuensi yang ditentukan organisas i] untuk pemantaua n dan [Penugasa n: frekuensi yang ditentukan organisas i] untuk penilaian yang mendukung pemantauan tersebut	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantaua n berkelanjutan dan menerapkan program pemantauan berkelanj utan yang meliputi: a. Pembentuk an [Penugasa n: metrik yang ditentukan organisas i] untuk dipantau; b. Pembentuk an [Penugasan: frekuensi yang ditentukan organisas i] untuk pemantaua n dan [Penugasa n: frekuensi yang ditentukan organisas i] untuk penilaian yang mendukung pemantauan tersebut	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteks i aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantauan berkelanjutan dan menerapkan program pemantauan berkelanjutan yang meliputi: a. Pembentukan [Penugasan: metrik yang ditentukan organisasi] untuk dipantau; b. Pembentukan [Penugasan: frekuensi yang ditentukan organisasi] untuk pemantauan dan [Penugasan: frekuensi yang ditentukan organisasi] untuk penilaian yang mendukung pemantauan tersebut	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantauan berkelanjutan dan menerapkan program pemantauan berkelanjutan yang meliputi: a. Pembentukan [Penugasan: metrik yang ditentukan organisasi] untuk dipantau; b. Pembentukan [Penugasan: frekuensi yang ditentukan organisasi] untuk pemantauan dan [Penugasan: frekuensi yang ditentukan organisasi] untuk penilaian yang mendukung pemantauan tersebut	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantaua n berkelanjutan dan menerapkan program pemantauan berkelanj utan yang meliputi: a. Pembentuk an [Penugasa n: metrik yang ditentukan organisas i] untuk dipantau; b. Pembentuk an [Penugasan: frekuensi yang ditentukan organisas i] untuk pemantaua n dan [Penugasa n: frekuensi yang ditentukan organisas i] untuk penilaian yang mendukung pemantauan tersebut	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantaua n berkelanjutan dan menerapkan program pemantauan berkelanj utan yang meliputi: a. Pembentuk an [Penugasa n: metrik yang ditentukan organisas i] untuk dipantau; b. Pembentuk an [Penugasan: frekuensi yang ditentukan organisas i] untuk pemantaua n dan [Penugasa n: frekuensi yang ditentukan organisas i] untuk penilaian yang mendukung pemantauan tersebut	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantauan berkelanjutan dan menerapkan program pemantauan berkelanjutan yang meliputi: a. Pembentukan [Penugasan: metrik yang ditentukan organisasi] untuk dipantau; b. Pembentukan [Penugasan: frekuensi yang ditentukan organisasi] untuk pemantauan dan [Penugasan: frekuensi yang ditentukan organisasi] untuk penilaian yang mendukung pemantauan tersebut	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizink an, memblokir, atau menghitung permintaa n web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindung inya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigurasi dasar saat ini dari sistem informasi.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigurasi dasar saat ini dari sistem informasi.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigurasi dasar saat ini dari sistem informasi.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigurasi dasar saat ini dari sistem informasi.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigurasi dasar saat ini dari sistem informasi.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigurasi dasar saat ini dari sistem informasi.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	sagemaker-notebook -no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/ 0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigurasi dasar saat ini dari sistem informasi.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	ec2- volume-inuse-check	Aturan ini memastika n bahwa volume Amazon Elastic Block Store yang dilampirk an ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentika n, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigurasi dasar saat ini dari sistem informasi.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigurasi dasar saat ini dari sistem informasi.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurk an ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
CM-7 (a)	Organisasi: a. Mengkonfigurasi sistem informasi untuk hanya menyediakan kemampuan penting.	ec2- instance-profile-a ttached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirk an profil instans ke instans Anda dapat membantu pengelola an hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-7 (a)	Organisasi: a. Mengkonfigurasi sistem informasi untuk hanya menyediakan kemampuan penting.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-7 (a)	Organisasi: a. Mengkonfigurasi sistem informasi untuk hanya menyediakan kemampuan penting.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-8 (1)	Organisasi memperbarui inventaris komponen sistem informasi sebagai bagian integral dari instalasi komponen, penghapusan, dan pembaruan sistem informasi.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-8 (1)	Organisasi memperbarui inventaris komponen sistem informasi sebagai bagian integral dari instalasi komponen, penghapusan, dan pembaruan sistem informasi.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-8 (3) (a)	Organisasi: a. Menggunakan mekanisme otomatis secara terus menerus, menggunakan mekanisme otomatis dengan penundaan maksimum lima menit dalam deteksi, untuk mendeteks i keberadaan komponen perangkat keras, perangkat lunak, dan firmware yang tidak sah dalam sistem informasi	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-8 (3) (a)	Organisasi: a. Menggunakan mekanisme otomatis secara terus menerus, menggunakan mekanisme otomatis dengan penundaan maksimum lima menit dalam deteksi, untuk mendeteks i keberadaan komponen perangkat keras, perangkat lunak, dan firmware yang tidak sah dalam sistem informasi	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventari s platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-8 (3) (a)	Organisasi: a. Menggunakan mekanisme otomatis secara terus menerus, menggunakan mekanisme otomatis dengan penundaan maksimum lima menit dalam deteksi, untuk mendeteks i keberadaan komponen perangkat keras, perangkat lunak, dan firmware yang tidak sah dalam sistem informasi	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-8 (3) (a)	Organisasi: a. Menggunakan mekanisme otomatis secara terus menerus, menggunakan mekanisme otomatis dengan penundaan maksimum lima menit dalam deteksi, untuk mendeteks i keberadaan komponen perangkat keras, perangkat lunak, dan firmware yang tidak sah dalam sistem informasi	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem informasi (inkremental harian; mingguan penuh).	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem informasi (inkremental harian; mingguan penuh).	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem informasi (inkremental harian; mingguan penuh).	dynamodb-resources-protected-by-rencana cadangan	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem informasi (inkremental harian; mingguan penuh).	ebs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem informasi (inkremental harian; mingguan penuh).	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem informasi (inkremental harian; mingguan penuh).	efs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem informasi (inkremental harian; mingguan penuh).	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem informasi (inkremental harian; mingguan penuh).	rds-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Relational Database Service (Amazon RDS) Anda merupakan AWS bagian dari paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem informasi (inkremental harian; mingguan penuh).	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem informasi (inkremental harian; mingguan penuh).	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem informasi (inkremental harian; mingguan penuh).	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem informasi (inkremental harian; mingguan penuh).	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem informasi (inkremental harian; mingguan penuh).	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem informasi (inkremental harian; mingguan penuh).	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	dynamodb-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	ebs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	efs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	rds-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Relational Database Service (Amazon RDS) Anda merupakan AWS bagian dari paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2 (1) (2)	(1) Sistem informasi menerapkan otentikasi multifaktor untuk akses jaringan ke akun istimewa. (2) Sistem informasi menerapkan otentikasi multifaktor untuk akses jaringan ke akun yang tidak memiliki hak istimewa.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2 (1) (2)	(1) Sistem informasi menerapkan otentikasi multifaktor untuk akses jaringan ke akun istimewa. (2) Sistem informasi menerapkan otentikasi multifaktor untuk akses jaringan ke akun yang tidak memiliki hak istimewa.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2 (1) (2)	(1) Sistem informasi menerapkan otentikasi multifaktor untuk akses jaringan ke akun istimewa. (2) Sistem informasi menerapkan otentikasi multifaktor untuk akses jaringan ke akun yang tidak memiliki hak istimewa.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2 (1) (2)	(1) Sistem informasi menerapkan otentikasi multifaktor untuk akses jaringan ke akun istimewa. (2) Sistem informasi menerapkan otentikasi multifaktor untuk akses jaringan ke akun yang tidak memiliki hak istimewa.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2 (1)	(1) Sistem informasi menerapkan otentikasi multifaktor untuk akses jaringan ke akun istimewa.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2 (1)	(1) Sistem informasi menerapkan otentikasi multifaktor untuk akses jaringan ke akun istimewa.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2 (1)	(1) Sistem informasi menerapkan otentikasi multifaktor untuk akses jaringan ke akun istimewa.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2 (1)	(1) Sistem informasi menerapkan otentikasi multifaktor untuk akses jaringan ke akun istimewa.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2	Sistem informasi secara unik mengidentifikasi dan mengotentikasi pengguna organisasi (atau proses yang bertindak atas nama pengguna organisasi).	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2	Sistem informasi secara unik mengidentifikasi dan mengotentikasi pengguna organisasi (atau proses yang bertindak atas nama pengguna organisasi).	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-5 (1) (a) (d) (e)	Sistem informasi , untuk otentikasi berbasis kata sandi: a. Menegakkan kompleksitas kata sandi minimum [Penugasan: persyaratan yang ditentukan organisasi untuk sensitivitas huruf besar, jumlah karakter, campuran huruf besar, huruf kecil, angka, dan karakter khusus, termasuk persyaratan minimum untuk setiap jenis]; d. Menegakkan batasan masa pakai minimum dan maksimum kata sandi [Penugasan: angka yang ditentukan organisasi untuk minimum seumur hidup, maksimum seumur hidup]; e. Melarang penggunaan kembali kata sandi selama 24 generasi	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-5 (4)	Organisasi menggunakan alat otomatis untuk menentukan apakah autentikator kata sandi cukup kuat untuk memenuhi [Penugasan: persyaratan yang ditentukan organisasi].	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-5 (7)	Organisasi memastikan bahwa autentikator statis yang tidak terenkripsi tidak disematkan dalam aplikasi atau skrip akses atau disimpan pada tombol fungsi.	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild. Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-4 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung proses penanganan insiden.	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-4 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung proses penanganan insiden.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-4 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung proses penanganan insiden.	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-4 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung proses penanganan insiden.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-4 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung proses penanganan insiden.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-6 (1)	Organisasi ini menggunakan mekanisme otomatis untuk membantu pelaporan insiden keamanan.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-6 (1)	Organisasi ini menggunakan mekanisme otomatis untuk membantu pelaporan insiden keamanan.	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-6 (1)	Organisasi ini menggunakan mekanisme otomatis untuk membantu pelaporan insiden keamanan.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-7 (1)	Organisasi ini menggunakan mekanisme otomatis untuk meningkat kan ketersediaan informasi dan dukungan terkait respons insiden.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-7 (1)	Organisasi ini menggunakan mekanisme otomatis untuk meningkat kan ketersediaan informasi dan dukungan terkait respons insiden.	guardduty-non-arch ived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasark an tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunak an klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSe v (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratk an oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-7 (1)	Organisasi ini menggunakan mekanisme otomatis untuk meningkat kan ketersediaan informasi dan dukungan terkait respons insiden.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RA-5 (1)	Organisasi ini menggunakan alat pemindaian kerentana n yang mencakup kemampuan untuk dengan mudah memperbarui kerentanan sistem informasi yang akan dipindai. Panduan Tambahan: Kerentanan yang akan dipindai perlu segera diperbaru i saat kerentana n baru ditemukan , diumumkan, dan metode pemindaia n dikembangkan. Proses pembaruan ini membantu memastika n bahwa potensi kerentanan dalam sistem informasi diidentifikasi dan ditangani secepat mungkin. Kontrol terkait: SI-3, SI-7.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RA-5 (1)	Organisasi ini menggunakan alat pemindaian kerentanan yang mencakup kemampuan untuk dengan mudah memperbarui kerentanan sistem informasi yang akan dipindai. Panduan Tambahan: Kerentanan yang akan dipindai perlu segera diperbarui saat kerentanan baru ditemukan, diumumkan, dan metode pemindaian dikembangkan. Proses pembaruan ini membantu memastikan bahwa potensi kerentanan dalam sistem informasi diidentifikasi dan ditangani secepat mungkin. Kontrol terkait: SI-3, SI-7.	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan: rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RA-5 (1)	Organisasi ini menggunakan alat pemindaian kerentana n yang mencakup kemampuan untuk dengan mudah memperbarui kerentanan sistem informasi yang akan dipindai. Panduan Tambahan: Kerentanan yang akan dipindai perlu segera diperbaru i saat kerentana n baru ditemukan , diumumkan, dan metode pemindaia n dikembangkan. Proses pembaruan ini membantu memastika n bahwa potensi kerentanan dalam sistem informasi diidentifikasi dan ditangani secepat mungkin. Kontrol terkait: SI-3, SI-7.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RA-5	Organisasi: a. Memindai kerentanan dalam sistem informasi dan aplikasi yang dihosting setiap bulan [operasi system/infrastructure; monthly web applications and databases] and when new vulnerabilities potentially affecting the system/applications diidentifikasi dan dilaporkan; b. Menggunakan alat dan teknik pemindaian kerentanan yang memfasilitasi interoperabilitas antar alat dan mengotomatiskan bagian dari proses manajemen kerentanan dengan menggunakan standar untuk: 1. Menghitung platform, kelemahan perangkat lunak, dan konfigurasi yang tidak tepat; 2. Memformat daftar periksa dan prosedur pengujian; dan 3. Mengukur dampak kerentana	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan: rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	n; c. Menganalisis laporan pemindaian kerentanan dan hasil dari penilaian kontrol keamanan; d. Memperbaiki kerentanan yang sah: kerentanan berisiko tinggi dikurangi dalam waktu tiga puluh (30) hari sejak tanggal penemuan; kerentanan risiko sedang dikurangi dalam sembilan puluh (90) hari sejak tanggal penemuan; kerentanan risiko rendah dikurangi dalam seratus delapan puluh (180) hari sejak tanggal penemuan, sesuai dengan penilaian risiko organisasi; dan e. Membagikan informasi yang diperoleh dari proses pemindaian kerentanan dan penilaian kontrol keamanan dengan [Penugasan: personel atau peran yang ditentukan organisasi] untuk		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	membantu menghilangkan kerentanan serupa dalam sistem informasi lain (yaitu, kelemahan atau kekurangan sistemik).		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RA-5	Organisasi: a. Memindai kerentana n dalam sistem informasi dan aplikasi yang dihosting [Penugasan: frekuensi yang ditentukan organisasi diidentif ikasi dan dilaporka n; and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/application s b. Menggunak an alat dan teknik pemindaian kerentana n yang memfasilitasi interoperabilitas antar alat dan mengotoma tiskan bagian dari proses manajemen kerentanan dengan menggunakan standar untuk: 1. Menghitung platform, kelemahan perangkat lunak, dan konfigurasi yang tidak tepat; 2. Memformat daftar periksa dan prosedur pengujian ; dan 3. Mengukur	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dampak kerentana n; c. Menganalisis laporan pemindaia n kerentanan dan hasil dari penilaian kontrol keamanan; d. Memulihkan kerentanan yang sah [Penugasa n: waktu respons yang ditentukan organisasi], sesuai dengan penilaian risiko organisasi; dan e. Membagika n informasi yang diperoleh dari proses pemindaian kerentana n dan penilaian kontrol keamanan dengan [Penugasa n: personel atau peran yang ditentuka n organisasi] untuk membantu menghilan gkan kerentanan serupa dalam sistem informasi lain (yaitu, kelemahan atau kekurangan sistemik).		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-3 (a)	Organisasi: a. Mengelola sistem informasi menggunakan [Penugasan: siklus hidup pengembangan sistem yang ditentukan organisasi] yang menggabungkan pertimbangan keamanan informasi.	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild . Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-3 (a)	Organisasi: a. Mengelola sistem informasi menggunakan [Penugasan: siklus hidup pengembangan sistem yang ditentukan organisasi] yang menggabungkan pertimbangan keamanan informasi.	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredenal masuk dalam lingkungan proyek Codebuild . AWS Gunakan OAuth alih-alih token akses pribadi atau kredensi masuk untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-3 (a)	Organisasi: a. Mengelola sistem informasi menggunakan [Penugasan: siklus hidup pengembangan sistem yang ditentukan organisasi] yang menggabungkan pertimbangan keamanan informasi.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-10	Organisasi membutuhkan pengembang sistem informasi, komponen sistem, atau layanan sistem informasi untuk: a. Melakukan manajemen konfigurasi selama pengembangan sistem, komponen, atau layanan, implementasi, DAN operasi; b. Mendokumentasikan, mengelola, dan mengontrol integritas perubahan pada [Penugasan: item konfigurasi yang ditentukan organisasi di bawah manajemen konfigurasi]; c. Menerapkan hanya perubahan yang disetujui organisasi pada sistem, komponen, atau layanan; d. Mendokumentasikan perubahan yang disetujui pada sistem, komponen, atau layanan dan potensi dampak keamanan	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan: rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dari perubahan tersebut; dan e. Lacak kelemahan keamanan dan resolusi cacat dalam sistem, komponen, atau layanan dan laporkan temuan ke [Penugasan: personel yang ditentukan organisasi].		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-10	Organisasi membutuhkan pengembang sistem informasi, komponen sistem, atau layanan sistem informasi untuk: a. Melakukan manajemen konfigura si selama pengemban gan sistem, komponen, atau layanan, implement asi, DAN operasi; b. Mendokume ntasikan, mengelola , dan mengontrol integritas perubahan pada [Penugasa n: item konfigura si yang ditentukan organisasi di bawah manajemen konfigura si]; c. Menerapkan hanya perubahan yang disetujui organisasi pada sistem, komponen, atau layanan; d. Mendokumentasikan perubahan yang disetujui pada sistem, komponen, atau layanan dan potensi dampak keamanan	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dari perubahan tersebut; dan e. Lacak kelemahan keamanan dan resolusi cacat dalam sistem, komponen, atau layanan dan laporkan temuan ke [Penugasan: personel yang ditentukan organisasi].		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-10	Organisasi membutuhkan pengembang sistem informasi, komponen sistem, atau layanan sistem informasi untuk: a. Melakukan manajemen konfigura si selama pengemban gan sistem, komponen, atau layanan, implement asi, DAN operasi; b. Mendokume ntasikan, mengelola , dan mengontrol integritas perubahan pada [Penugasa n: item konfigura si yang ditentukan organisasi di bawah manajemen konfigura si]; c. Menerapkan hanya perubahan yang disetujui organisasi pada sistem, komponen, atau layanan; d. Mendokumentasikan perubahan yang disetujui pada sistem, komponen, atau layanan dan potensi dampak keamanan	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dari perubahan tersebut; dan e. Lacak kelemahan keamanan dan resolusi cacat dalam sistem, komponen, atau layanan dan laporkan temuan ke [Penugasan: personel yang ditentukan organisasi].		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-10	Organisasi membutuhkan pengembang sistem informasi, komponen sistem, atau layanan sistem informasi untuk: a. Melakukan manajemen konfigura si selama pengemban gan sistem, komponen, atau layanan, implement asi, DAN operasi; b. Mendokume ntasikan, mengelola , dan mengontrol integritas perubahan pada [Penugasa n: item konfigura si yang ditentukan organisasi di bawah manajemen konfigura si]; c. Menerapkan hanya perubahan yang disetujui organisasi pada sistem, komponen, atau layanan; d. Mendokumentasikan perubahan yang disetujui pada sistem, komponen, atau layanan dan potensi dampak keamanan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dari perubahan tersebut; dan e. Lacak kelemahan keamanan dan resolusi cacat dalam sistem, komponen, atau layanan dan laporkan temuan ke [Penugasan: personel yang ditentukan organisasi].		
SC-2	Sistem informasi memisahkan fungsionalitas pengguna (termasuk layanan antarmuka pengguna) dari fungsi manajemen sistem informasi.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-2	Sistem informasi memisahkan fungsionalitas pengguna (termasuk layanan antarmuka pengguna) dari fungsi manajemen sistem informasi.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-2	Sistem informasi memisahkan fungsionalitas pengguna (termasuk layanan antarmuka pengguna) dari fungsi manajemen sistem informasi.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-2	Sistem informasi memisahkan fungsionalitas pengguna (termasuk layanan antarmuka pengguna) dari fungsi manajemen sistem informasi.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-2	Sistem informasi memisahkan fungsionalitas pengguna (termasuk layanan antarmuka pengguna) dari fungsi manajemen sistem informasi.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	s3- account-level-publ ic-access -blok-per iodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Organisasi: (a) Menerapkan antarmuka terkelola untuk setiap layanan telekomunikasi eksternal; (b) Menetapkan kebijakan arus lalu lintas untuk setiap antarmuka yang dikelola; (c) Melindungi kerahasiaan dan integritas informasi yang dikirimkan di setiap antarmuka; (d) Mendokumentasikan setiap pengecualian ke kebijakan arus lalu lintas dengan kebutuhan pendukung. mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business Panduan	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Tambahan: Kontrol terkait: SC-8.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Organisasi: (a) Menerapkan antarmuka terkelola untuk setiap layanan telekomunikasi eksternal; (b) Menetapkan kebijakan arus lalu lintas untuk setiap antarmuka yang dikelola; (c) Melindungi kerahasiaan dan integritas informasi yang dikirimkan di setiap antarmuka; (d) Mendokumentasikan setiap pengecualian ke kebijakan arus lalu lintas dengan kebutuhan pendukung. mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business Panduan	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Tambahan: Kontrol terkait: SC-8.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Organisasi: (a) Menerapkan antarmuka terkelola untuk setiap layanan telekomunikasi eksternal; (b) Menetapkan kebijakan arus lalu lintas untuk setiap antarmuka yang dikelola; (c) Melindungi kerahasiaan dan integritas informasi yang dikirimkan di setiap antarmuka; (d) Mendokumentasikan setiap pengecualian ke kebijakan arus lalu lintas dengan kebutuhan pendukung. mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business Panduan	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Tambahan: Kontrol terkait: SC-8.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Organisasi: (a) Menerapkan antarmuka terkelola untuk setiap layanan telekomunikasi eksternal; (b) Menetapkan kebijakan arus lalu lintas untuk setiap antarmuka yang dikelola; (c) Melindungi kerahasiaan dan integritas informasi yang dikirimkan di setiap antarmuka; (d) Mendokumentasikan setiap pengecualian ke kebijakan arus lalu lintas dengan kebutuhan pendukung. mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business Panduan	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Tambahan: Kontrol terkait: SC-8.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Organisasi: (a) Menerapkan antarmuka terkelola untuk setiap layanan telekomunikasi eksternal; (b) Menetapkan kebijakan arus lalu lintas untuk setiap antarmuka yang dikelola; (c) Melindungi kerahasiaan dan integritas informasi yang dikirimkan di setiap antarmuka; (d) Mendokumentasikan setiap pengecualian ke kebijakan arus lalu lintas dengan kebutuhan pendukung. mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business Panduan	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Tambahan: Kontrol terkait: SC-8.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Organisasi: (a) Menerapkan antarmuka terkelola untuk setiap layanan telekomunikasi eksternal; (b) Menetapkan kebijakan arus lalu lintas untuk setiap antarmuka yang dikelola; (c) Melindungi kerahasiaan dan integritas informasi yang dikirimkan di setiap antarmuka; (d) Mendokumentasikan setiap pengecualian ke kebijakan arus lalu lintas dengan kebutuhan pendukung. mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business Panduan	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Tambahan: Kontrol terkait: SC-8.		
SC-7 (5)	Sistem informasi pada antarmuka terkelola menyangkal lalu lintas komunikasi jaringan secara default dan memungkinkan lalu lintas komunikas i jaringan dengan pengecualian (yaitu, menolak semua, izin dengan pengecual ian). Panduan Tambahan: Peningkat an kontrol ini berlaku untuk lalu lintas komunikasi jaringan masuk dan keluar. Kebijakan lalu lintas komunikasi permit-by -exception jaringan yang menyangkal semua memastika n bahwa hanya koneksi yang penting dan disetujui yang diizinkan.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/ 0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigurasi ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8 (1)	Sistem informasi menerapkan mekanisme kriptografi untuk [Seleksi (satu atau lebih): mencegah pengungkapan informasi yang tidak sah; mendeteksi perubahan informasi] selama transmisi kecuali dilindungi oleh [Penugasan: perlindungan fisik alternatif yang ditentukan organisasi].	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8 (1)	Sistem informasi menerapkan mekanisme kriptografi untuk [Seleksi (satu atau lebih): mencegah pengungkapan informasi yang tidak sah; mendeteksi perubahan informasi] selama transmisi kecuali dilindungi oleh [Penugasan: perlindungan fisik alternatif yang ditentukan organisasi].	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
SC-8 (1)	Sistem informasi menerapkan mekanisme kriptografi untuk [Seleksi (satu atau lebih): mencegah pengungkapan informasi yang tidak sah; mendeteksi perubahan informasi] selama transmisi kecuali dilindungi oleh [Penugasan: perlindungan fisik alternatif yang ditentukan organisasi].	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8 (1)	Sistem informasi menerapkan mekanisme kriptografi untuk [Seleksi (satu atau lebih): mencegah pengungkapan informasi yang tidak sah; mendeteksi perubahan informasi] selama transmisi kecuali dilindungi oleh [Penugasan: perlindungan fisik alternatif yang ditentukan organisasi].	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-8 (1)	Sistem informasi menerapkan mekanisme kriptografi untuk [Seleksi (satu atau lebih): mencegah pengungkapan informasi yang tidak sah; mendeteksi perubahan informasi] selama transmisi kecuali dilindungi oleh [Penugasan: perlindungan fisik alternatif yang ditentukan organisasi].	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8 (1)	Sistem informasi menerapkan mekanisme kriptografi untuk [Seleksi (satu atau lebih): mencegah pengungkapan informasi yang tidak sah; mendeteksi perubahan informasi] selama transmisi kecuali dilindungi oleh [Penugasan: perlindungan fisik alternatif yang ditentukan organisasi].	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-8 (1)	Sistem informasi menerapkan mekanisme kriptografi untuk [Seleksi (satu atau lebih): mencegah pengungkapan informasi yang tidak sah; mendeteksi perubahan informasi] selama transmisi kecuali dilindungi oleh [Penugasan: perlindungan fisik alternatif yang ditentukan organisasi].	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8	Sistem informasi melindungi kerahasia an DAN integrita s informasi yang dikirimkan.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-n ode enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkrip si memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8	Sistem informasi melindungi kerahasia an DAN integrita s informasi yang dikirimkan.	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
SC-8	Sistem informasi melindungi kerahasia an DAN integrita s informasi yang dikirimkan.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8	Sistem informasi melindungi kerahasiaan DAN integritas informasi yang dikirimkan.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-8	Sistem informasi melindungi kerahasiaan DAN integritas informasi yang dikirimkan.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8	Sistem informasi melindungi kerahasia an DAN integrita s informasi yang dikirimkan.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-8	Sistem informasi melindungi kerahasia an DAN integrita s informasi yang dikirimkan.	s3- bucket-ssl-request s-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-12	Organisasi menetapkan dan mengelola kunci kriptografi untuk kriptografi yang diperlukan yang digunakan dalam sistem informasi sesuai dengan [Penugasan: persyaratan yang ditentukan organisasi untuk pembuatan kunci, distribusi, penyimpanan, akses, dan penghancuran].	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.
SC-12	Organisasi menetapkan dan mengelola kunci kriptografi untuk kriptografi yang diperlukan yang digunakan dalam sistem informasi sesuai dengan [Penugasan: persyaratan yang ditentukan organisasi untuk pembuatan kunci, distribusi, penyimpanan, akses, dan penghancuran].	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-12	Organisasi menetapkan dan mengelola kunci kriptografi untuk kriptografi yang diperlukan yang digunakan dalam sistem informasi sesuai dengan [Penugasan: persyaratan yang ditentukan organisasi untuk pembuatan kunci, distribusi, penyimpanan, akses, dan penghancuran].	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13	Sistem informasi mengimplementasikan kriptografi yang divalidasi FIPS atau disetujui NSA sesuai dengan hukum federal, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar yang berlaku.	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.
SC-13	Sistem informasi mengimplementasikan kriptografi yang divalidasi FIPS atau disetujui NSA sesuai dengan hukum federal, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar yang berlaku.	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13	Sistem informasi mengimplementasikan kriptografi yang divalidasi FIPS atau disetujui NSA sesuai dengan hukum federal, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar yang berlaku.	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-13	Sistem informasi mengimplementasikan kriptografi yang divalidasi FIPS atau disetujui NSA sesuai dengan hukum federal, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar yang berlaku.	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13	Sistem informasi mengimplementasikan kriptografi yang divalidasi FIPS atau disetujui NSA sesuai dengan hukum federal, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar yang berlaku.	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13	Sistem informasi mengimplementasikan kriptografi yang divalidasi FIPS atau disetujui NSA sesuai dengan hukum federal, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar yang berlaku.	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-23	Sistem informasi melindungi keaslian sesi komunikasi.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-23	Sistem informasi melindungi keaslian sesi komunikasi.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-23	Sistem informasi melindungi keaslian sesi komunikasi.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-23	Sistem informasi melindungi keaslian sesi komunikasi.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
SC-23	Sistem informasi melindungi keaslian sesi komunikasi.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-23	Sistem informasi melindungi keaslian sesi komunikasi.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28	Sistem informasi melindungi kerahasia an DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrai l jejak Anda.
SC-28	Sistem informasi melindungi kerahasia an DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
SC-28	Sistem informasi melindungi kerahasia an DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2 (2)	Organisasi menggunak an mekanisme otomatis setidakny a setiap bulan untuk menentukan keadaan komponen sistem informasi sehubunga n dengan remediasi cacat.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2 (2)	Organisasi menggunak an mekanisme otomatis setidakny a setiap bulan untuk menentukan keadaan komponen sistem informasi sehubunga n dengan remediasi cacat.	ec2- -periksa managedinstance-as sociation-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventari s platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2 (2)	Organisasi menggunak an mekanisme otomatis setidakny a setiap bulan untuk menentukan keadaan komponen sistem informasi sehubunga n dengan remediasi cacat.	ec2- -periksa managedinstance-pa tch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
SI-2 (2)	Organisasi menggunak an mekanisme otomatis setidakny a setiap bulan untuk menentukan keadaan komponen sistem informasi sehubunga n dengan remediasi cacat.	elastic-beanstalk-managed-updates-di aktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-3	Organisasi: a. Menggunakan mekanisme perlindungan kode berbahaya pada titik masuk dan keluar sistem informasi untuk mendeteksi dan memberantas kode berbahaya ; b. Memperbarui mekanisme perlindungan kode berbahaya setiap kali rilis baru tersedia sesuai dengan kebijakan dan prosedur manajemen konfigurasi organisasi; c. Mengkonfigurasi mekanisme perlindungan kode berbahaya ke: 1. Lakukan pemindaian berkala dari sistem informasi [Penugasan: frekuensi yang ditentukan organisasi] dan pemindaian file secara real-time dari sumber eksternal di [Seleksi (satu atau lebih); titik akhir; entry/exit points] as the files	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild . Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	are downloaded, opened, or executed in accordance with organizational security policy; and 2. [Selection(one or more): block malicious code; quarantine malicious code; send alert to administr ator; [Assignment: organization-defined action]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availabil ity of the information system. Supplemental Guidance: Informati on system entry and exit points include, for example, firewalls , electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers , and mobile devices.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats(for example, UUENCODE, Unicode), contained within compresse d or hidden files, or hidden in files using steganogr aphy. Malicious code can be transport ed by different means including, for example, web accesses, electroni c mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitat ion of information system vulnerabi lities. Malicious code protection mechanisms include, for example, anti-viru s signature definitio ns and reputation-based technologies.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example,		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or tindakan jaringan dalam menanggapi deteksi kejahatan ketika mencoba membuka atau mengeksekusi file. Kontrol terkait: CM-3, MP-2, SA-4, SA-8,		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7. Referensi : Publikasi Khusus NIST 800-83.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-3	Organisasi: a. Menggunakan mekanisme perlindungan kode berbahaya pada titik masuk dan keluar sistem informasi untuk mendeteksi dan memberantas kode berbahaya ; b. Memperbarui mekanisme perlindungan kode berbahaya setiap kali rilis baru tersedia sesuai dengan kebijakan dan prosedur manajemen konfigurasi organisasi; c. Mengkonfigurasi mekanisme perlindungan kode berbahaya ke: 1. Lakukan pemindaian berkala dari sistem informasi [Penugasan: frekuensi yang ditentukan organisasi] dan pemindaian file secara real-time dari sumber eksternal di [Seleksi (satu atau lebih); titik akhir; entry/exit points] as the files	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredenal masuk dalam lingkungan proyek Codebuild . AWS Gunakan OAuth alih-alih token akses pribadi atau kredensi masuk untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	are downloaded, opened, or executed in accordance with organizational security policy; and 2. [Selection(one or more): block malicious code; quarantine malicious code; send alert to administr ator; [Assignment: organization-defined action]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availabil ity of the information system. Supplemental Guidance: Informati on system entry and exit points include, for example, firewalls , electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers , and mobile devices.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats(for example, UUENCODE, Unicode), contained within compresse d or hidden files, or hidden in files using steganogr aphy. Malicious code can be transport ed by different means including, for example, web accesses, electroni c mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitat ion of information system vulnerabi lities. Malicious code protection mechanisms include, for example, anti-viru s signature definitio ns and reputation-based technologies.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example,		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	secure coding practices, configura tion managemen t and control, trusted procureme nt processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted . For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or tindakan jaringan dalam menanggap i deteksi kejahatan ketika mencoba membuka atau mengeksekusi file. Kontrol terkait: CM-3, MP-2, SA-4, SA-8,		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7. Referensi : Publikasi Khusus NIST 800-83.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-3	Organisasi: a. Menggunakan mekanisme perlindungan kode berbahaya pada titik masuk dan keluar sistem informasi untuk mendeteksi dan memberantas kode berbahaya ; b. Memperbarui mekanisme perlindungan kode berbahaya setiap kali rilis baru tersedia sesuai dengan kebijakan dan prosedur manajemen konfigurasi organisasi; c. Mengkonfigurasi mekanisme perlindungan kode berbahaya ke: 1. Lakukan pemindaian berkala dari sistem informasi [Penugasan: frekuensi yang ditentukan organisasi] dan pemindaian file secara real-time dari sumber eksternal di [Seleksi (satu atau lebih); titik akhir; entry/exit points] as the files	ecs-task-definition-memory-batas-keras	Membatasi memori maksimum yang tersedia untuk penampung Amazon Elastic Container Service (ECS) memastikan bahwa penggunaan sumber daya Anda tidak dapat disalahgunakan jika terjadi akses berbahaya ke kontainer Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	are downloaded, opened, or executed in accordance with organizational security policy; and 2. [Selection(one or more): block malicious code; quarantine malicious code; send alert to administr ator; [Assignment: organization-defined action]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availabil ity of the information system. Supplemental Guidance: Informati on system entry and exit points include, for example, firewalls , electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers , and mobile devices.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats(for example, UUENCODE, Unicode), contained within compresse d or hidden files, or hidden in files using steganogr aphy. Malicious code can be transport ed by different means including, for example, web accesses, electroni c mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitat ion of information system vulnerabi lities. Malicious code protection mechanisms include, for example, anti-viru s signature definitio ns and reputation-based technologies.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example,		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or tindakan jaringan dalam menanggapi deteksi kejahatan ketika mencoba membuka atau mengeksekusi file. Kontrol terkait: CM-3, MP-2, SA-4, SA-8,		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7. Referensi : Publikasi Khusus NIST 800-83.		
SI-4 (1)	Organisasi menghubungkan dan mengonfigurasi alat deteksi intrusi individu ke dalam sistem deteksi intrusi di seluruh sistem informasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (2)	Organisasi ini menggunakan alat otomatis untuk mendukung analisis peristiwa yang hampir real-time.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (2)	Organisasi ini menggunakan alat otomatis untuk mendukung analisis peristiwa yang hampir real-time.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (2)	Organisasi ini menggunakan alat otomatis untuk mendukung analisis peristiwa yang hampir real-time.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
SI-4 (2)	Organisasi ini menggunakan alat otomatis untuk mendukung analisis peristiwa yang hampir real-time.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (2)	Organisasi ini menggunakan alat otomatis untuk mendukung analisis peristiwa yang hampir real-time.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (2)	Organisasi ini menggunakan alat otomatis untuk mendukung analisis peristiwa yang hampir real-time.	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.
SI-4 (2)	Organisasi ini menggunakan alat otomatis untuk mendukung analisis peristiwa yang hampir real-time.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (2)	Organisasi ini menggunakan alat otomatis untuk mendukung analisis peristiwa yang hampir real-time.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (4)	Sistem informasi memantau lalu lintas komunikasi masuk dan keluar secara terus menerus untuk aktivitas atau kondisi yang tidak biasa atau tidak sah.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (4)	Sistem informasi memantau lalu lintas komunikasi masuk dan keluar secara terus menerus untuk aktivitas atau kondisi yang tidak biasa atau tidak sah.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (4)	Sistem informasi memantau lalu lintas komunikasi masuk dan keluar secara terus menerus untuk aktivitas atau kondisi yang tidak biasa atau tidak sah.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (4)	Sistem informasi memantau lalu lintas komunikasi masuk dan keluar secara terus menerus untuk aktivitas atau kondisi yang tidak biasa atau tidak sah.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (5)	Sistem informasi memperingatkan [Penugasan: personel atau peran yang ditentukan organisasi] ketika indikasi kompromi atau potensi kompromi berikut terjadi: [Penugasan: indikator kompromi yang ditentukan organisasi].	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (5)	Sistem informasi memperingatkan [Penugasan: personel atau peran yang ditentukan organisasi] ketika indikasi kompromi atau potensi kompromi berikut terjadi: [Penugasan: indikator kompromi yang ditentukan organisasi].	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (5)	Sistem informasi memperingatkan [Penugasan: personel atau peran yang ditentukan organisasi] ketika indikasi kompromi atau potensi kompromi berikut terjadi: [Penugasan: indikator kompromi yang ditentukan organisasi].	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (5)	Sistem informasi memperingatkan [Penugasan: personel atau peran yang ditentukan organisasi] ketika indikasi kompromi atau potensi kompromi berikut terjadi: [Penugasan: indikator kompromi yang ditentukan organisasi].	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (16)	Organisasi mengkorelasikan informasi dari alat pemantauan yang digunakan di seluruh sistem informasi.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (16)	Organisasi mengkorel asikan informasi dari alat pemantauan yang digunakan di seluruh sistem informasi.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (16)	Organisasi mengkorel asikan informasi dari alat pemantauan yang digunakan di seluruh sistem informasi.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
SI-4 (16)	Organisasi mengkorel asikan informasi dari alat pemantauan yang digunakan di seluruh sistem informasi.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteks i aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (16)	Organisasi mengkorel asikan informasi dari alat pemantauan yang digunakan di seluruh sistem informasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (16)	Organisasi mengkorelasikan informasi dari alat pemantauan yang digunakan di seluruh sistem informasi.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (a) (b) (c)	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1. Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2. Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c. Menyebarkan perangkat pemantauan: i. secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan (ii) di lokasi ad hoc dalam sistem untuk melacak jenis transaksi	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	tertentu yang menarik bagi organisasi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (a) (b) (c)	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1. Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2. Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c. Menyebarkan perangkat pemantauan: i. secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan (ii) di lokasi ad hoc dalam sistem untuk melacak jenis transaksi	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindungi nya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	tertentu yang menarik bagi organisasi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (a) (b) (c)	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1. Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2. Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c. Menyebarkan perangkat pemantauan: i. secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan (ii) di lokasi ad hoc dalam sistem untuk melacak jenis transaksi	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan: rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	tertentu yang menarik bagi organisasi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (a) (b) (c)	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1. Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2. Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c. Menyebarkan perangkat pemantauan: i. secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan (ii) di lokasi ad hoc dalam sistem untuk melacak jenis transaksi	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	tertentu yang menarik bagi organisasi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (a) (b) (c)	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1. Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2. Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c. Menyebarkan perangkat pemantauan: i. secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan (ii) di lokasi ad hoc dalam sistem untuk melacak jenis transaksi	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	tertentu yang menarik bagi organisasi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (a) (b) (c)	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1. Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2. Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c. Menyebarkan perangkat pemantauan: i. secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan (ii) di lokasi ad hoc dalam sistem untuk melacak jenis transaksi	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	tertentu yang menarik bagi organisasi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (a) (b) (c)	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1. Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2. Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c. Menyebarkan perangkat pemantauan: i. secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan (ii) di lokasi ad hoc dalam sistem untuk melacak jenis transaksi	cloudwatch-alarm-action-check	Amazon CloudWatch memperingatkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	tertentu yang menarik bagi organisasi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (a) (b) (c)	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1. Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2. Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c. Menyebarkan perangkat pemantauan: i. secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan (ii) di lokasi ad hoc dalam sistem untuk melacak jenis transaksi	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	tertentu yang menarik bagi organisasi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (a) (b) (c)	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1. Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2. Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c. Menyebarkan perangkat pemantauan: i. secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan (ii) di lokasi ad hoc dalam sistem untuk melacak jenis transaksi	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	tertentu yang menarik bagi organisasi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-5	Organisasi: a. Menerima peringatan, nasihat, dan arahan keamanan sistem informasi dari [Penugasan: organisasi eksternal yang ditentukan organisasi] secara berkelanjutan; b. Menghasilkan peringatan keamanan internal, nasihat, dan arahan yang dianggap perlu; c. Menyebarluaskan peringatan keamanan, nasihat, dan arahan ke: [Seleksi (satu atau lebih): [Penugasan: personel atau peran yang ditentukan organisasi]; [Penugasan: elemen yang ditentukan organisasi dalam organisasi]; [Penugasan: organisasi eksternal yang ditentukan organisasi]]; dan d. Menerapkan arahan keamanan sesuai dengan kerangka	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	waktu yang ditetapkan, atau memberi tahu organisasi penerbit tentang tingkat ketidakpatuhan. Panduan Tambahan: Tim Kesiapan Darurat Komputer Amerika Serikat (US-CERT) menghasilkan peringatan dan nasihat keamanan untuk menjaga kesadaran situasional di seluruh pemerintah federal. Arahan keamanan dikeluarkan oleh OMB atau organisasi lain yang ditunjuk dengan tanggung jawab dan wewenang untuk mengeluarkan arahan tersebut. Kepatuhan terhadap arahan keamanan sangat penting karena sifat kritis dari banyak arahan ini dan potensi efek samping langsung pada operasi dan aset organisasi, individu, organisasi lain, dan Bangsa		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	jika arahan tidak dilaksanakan pada waktu yang tepat. Organisasi eksternal termasuk, misalnya, mission/business partners, supply chain partners, external service providers, and other peer/supporting organisasi eksternal . Kontrol terkait: SI-2. Referensi: Publikasi Khusus NIST 800-40.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-5	Organisasi: a. Menerima peringatan, nasihat, dan arahan keamanan sistem informasi dari [Penugasan: organisasi eksternal yang ditentukan organisasi] secara berkelanjutan; b. Menghasilkan peringatan keamanan internal, nasihat, dan arahan yang dianggap perlu; c. Menyebarluaskan peringatan keamanan, nasihat, dan arahan ke: [Seleksi (satu atau lebih): [Penugasan: personel atau peran yang ditentukan organisasi]; [Penugasan: elemen yang ditentukan organisasi dalam organisasi]; [Penugasan: organisasi eksternal yang ditentukan organisasi]]; dan d. Menerapkan arahan keamanan sesuai dengan kerangka	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	waktu yang ditetapkan, atau memberi tahu organisasi penerbit tentang tingkat ketidakpatuhan. Panduan Tambahan: Tim Kesiapan Darurat Komputer Amerika Serikat (US-CERT) menghasilkan peringatan dan nasihat keamanan untuk menjaga kesadaran situasional di seluruh pemerintah federal. Arahan keamanan dikeluarkan oleh OMB atau organisasi lain yang ditunjuk dengan tanggung jawab dan wewenang untuk mengeluarkan arahan tersebut. Kepatuhan terhadap arahan keamanan sangat penting karena sifat kritis dari banyak arahan ini dan potensi efek samping langsung pada operasi dan aset organisasi, individu, organisasi lain, dan Bangsa		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	jika arahan tidak dilaksanakan pada waktu yang tepat. Organisasi eksternal termasuk, misalnya, mission/business partners, supply chain partners, external service providers, and other peer/supporting organisasi eksternal . Kontrol terkait: SI-2. Referensi: Publikasi Khusus NIST 800-40.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-5	Organisasi: a. Menerima peringatan, nasihat, dan arahan keamanan sistem informasi dari [Penugasan: organisasi eksternal yang ditentukan organisasi] secara berkelanjutan; b. Menghasilkan peringatan keamanan internal, nasihat, dan arahan yang dianggap perlu; c. Menyebarluaskan peringatan keamanan, nasihat, dan arahan ke: [Seleksi (satu atau lebih): [Penugasan: personel atau peran yang ditentukan organisasi]; [Penugasan: elemen yang ditentukan organisasi dalam organisasi]; [Penugasan: organisasi eksternal yang ditentukan organisasi]]; dan d. Menerapkan arahan keamanan sesuai dengan kerangka	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan: rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	waktu yang ditetapkan, atau memberi tahu organisasi penerbit tentang tingkat ketidakpatuhan. Panduan Tambahan: Tim Kesiapan Darurat Komputer Amerika Serikat (US-CERT) menghasilkan peringatan dan nasihat keamanan untuk menjaga kesadaran situasional di seluruh pemerintah federal. Arahan keamanan dikeluarkan oleh OMB atau organisasi lain yang ditunjuk dengan tanggung jawab dan wewenang untuk mengeluarkan arahan tersebut. Kepatuhan terhadap arahan keamanan sangat penting karena sifat kritis dari banyak arahan ini dan potensi efek samping langsung pada operasi dan aset organisasi, individu, organisasi lain, dan Bangsa		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	jika arahan tidak dilaksanakan pada waktu yang tepat. Organisasi eksternal termasuk, misalnya, mission/business partners, supply chain partners, external service providers, and other peer/supporting organisasi eksternal . Kontrol terkait: SI-2. Referensi: Publikasi Khusus NIST 800-40.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-5	Organisasi: a. Menerima peringatan, nasihat, dan arahan keamanan sistem informasi dari [Penugasan: organisasi eksternal yang ditentukan organisasi] secara berkelanjutan; b. Menghasilkan peringatan keamanan internal, nasihat, dan arahan yang dianggap perlu; c. Menyebarluaskan peringatan keamanan, nasihat, dan arahan ke: [Seleksi (satu atau lebih): [Penugasan: personel atau peran yang ditentukan organisasi]; [Penugasan: elemen yang ditentukan organisasi dalam organisasi]; [Penugasan: organisasi eksternal yang ditentukan organisasi]]; dan d. Menerapkan arahan keamanan sesuai dengan kerangka	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	waktu yang ditetapkan, atau memberi tahu organisasi penerbit tentang tingkat ketidakpatuhan. Panduan Tambahan: Tim Kesiapan Darurat Komputer Amerika Serikat (US-CERT) menghasilkan peringatan dan nasihat keamanan untuk menjaga kesadaran situasional di seluruh pemerintah federal. Arahan keamanan dikeluarkan oleh OMB atau organisasi lain yang ditunjuk dengan tanggung jawab dan wewenang untuk mengeluarkan arahan tersebut. Kepatuhan terhadap arahan keamanan sangat penting karena sifat kritis dari banyak arahan ini dan potensi efek samping langsung pada operasi dan aset organisasi, individu, organisasi lain, dan Bangsa		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	jika arahan tidak dilaksanakan pada waktu yang tepat. Organisasi eksternal termasuk, misalnya, mission/business partners, supply chain partners, external service providers, and other peer/supporting organisasi eksternal . Kontrol terkait: SI-2. Referensi: Publikasi Khusus NIST 800-40.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (1)	Sistem informasi melakukan pemeriksaan integritas keamanan peristiwa yang relevan setidaknya setiap bulan.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus, atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (1)	Sistem informasi melakukan pemeriksaan integritas keamanan peristiwa yang relevan setidaknya setiap bulan.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (1)	Sistem informasi melakukan pemeriksaan integritas keamanan peristiwa yang relevan setidaknya setiap bulan.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7	Organisasi menggunakan alat verifikasi integritas untuk mendeteksi perubahan yang tidak sah pada [Penugasan: perangkat lunak, firmware, dan informasi yang ditentukan organisasi].	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus, atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-11	Sistem informasi: a. Menghasilkan pesan kesalahan yang memberikan informasi yang diperlukan untuk tindakan korektif tanpa mengungkapkan informasi yang dapat dieksploitasi oleh musuh; dan b. Mengungkapkan pesan kesalahan hanya ke [Penugasan: personel atau peran yang ditentukan organisasi]. Panduan Tambahan: Organizations dengan hati-hati mempertimbangkan structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	attempts with passwords entered by mistake as the username, mission/business informasi yang dapat diperoleh dari (jika tidak dinyatakan secara eksplisit oleh) informasi yang direkam, dan informasi pribadi seperti nomor rekening, nomor jaminan sosial, dan nomor kartu kredit. Selain itu, pesan kesalahan dapat menyediak an saluran rahasia untuk mengirimkan informasi. Kontrol terkait: AU-2, AU-3, SC-31. Peningkatan Kontrol: Tidak ada. Referensi: Tidak ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-11	Sistem informasi: a. Menghasilkan pesan kesalahan yang memberikan informasi yang diperlukan untuk tindakan korektif tanpa mengungka pkan informasi yang dapat dieksploitasi oleh musuh; dan b. Mengungkapkan pesan kesalahan hanya ke [Penugasa n: personel atau peran yang ditentukan organisasi]. Panduan Tambahan: Organizat ions dengan hati-hati mempertimbangkan structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operation al requirements. Information that could be exploited by adversaries includes, for example, erroneous logon	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	attempts with passwords entered by mistake as the username, mission/business informasi yang dapat diperoleh dari (jika tidak dinyatakan secara eksplisit oleh) informasi yang direkam, dan informasi pribadi seperti nomor rekening, nomor jaminan sosial, dan nomor kartu kredit. Selain itu, pesan kesalahan dapat menyediak an saluran rahasia untuk mengirimkan informasi. Kontrol terkait: AU-2, AU-3, SC-31. Peningkatan Kontrol: Tidak ada. Referensi: Tidak ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-11	Sistem informasi: a. Menghasilkan pesan kesalahan yang memberikan informasi yang diperlukan untuk tindakan korektif tanpa mengungkapkan informasi yang dapat dieksploitasi oleh musuh; dan b. Mengungkapkan pesan kesalahan hanya ke [Penugasan: personel atau peran yang ditentukan organisasi]. Panduan Tambahan: Organizations dengan hati-hati mempertimbangkan structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	attempts with passwords entered by mistake as the username, mission/business informasi yang dapat diperoleh dari (jika tidak dinyatakan secara eksplisit oleh) informasi yang direkam, dan informasi pribadi seperti nomor rekening, nomor jaminan sosial, dan nomor kartu kredit. Selain itu, pesan kesalahan dapat menyediak an saluran rahasia untuk mengirimkan informasi. Kontrol terkait: AU-2, AU-3, SC-31. Peningkatan Kontrol: Tidak ada. Referensi: Tidak ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-11	Sistem informasi: a. Menghasilkan pesan kesalahan yang memberikan informasi yang diperlukan untuk tindakan korektif tanpa mengungka pkan informasi yang dapat dieksploitasi oleh musuh; dan b. Mengungkapkan pesan kesalahan hanya ke [Penugasa n: personel atau peran yang ditentukan organisasi]. Panduan Tambahan: Organizat ions dengan hati-hati mempertimbangkan structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operation al requirements. Information that could be exploited by adversaries includes, for example, erroneous logon	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	attempts with passwords entered by mistake as the username, mission/business informasi yang dapat diperoleh dari (jika tidak dinyatakan secara eksplisit oleh) informasi yang direkam, dan informasi pribadi seperti nomor rekening, nomor jaminan sosial, dan nomor kartu kredit. Selain itu, pesan kesalahan dapat menyediak an saluran rahasia untuk mengirimkan informasi. Kontrol terkait: AU-2, AU-3, SC-31. Peningkatan Kontrol: Tidak ada. Referensi: Tidak ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-11	Sistem informasi: a. Menghasilkan pesan kesalahan yang memberikan informasi yang diperlukan untuk tindakan korektif tanpa mengungkapkan informasi yang dapat dieksploitasi oleh musuh; dan b. Mengungkapkan pesan kesalahan hanya ke [Penugasan: personel atau peran yang ditentukan organisasi]. Panduan Tambahan: Organizations dengan hati-hati mempertimbangkan structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	attempts with passwords entered by mistake as the username, mission/business informasi yang dapat diperoleh dari (jika tidak dinyatakan secara eksplisit oleh) informasi yang direkam, dan informasi pribadi seperti nomor rekening, nomor jaminan sosial, dan nomor kartu kredit. Selain itu, pesan kesalahan dapat menyediak an saluran rahasia untuk mengirimkan informasi. Kontrol terkait: AU-2, AU-3, SC-31. Peningkatan Kontrol: Tidak ada. Referensi: Tidak ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-11	Sistem informasi: a. Menghasilkan pesan kesalahan yang memberikan informasi yang diperlukan untuk tindakan korektif tanpa mengungka pkan informasi yang dapat dieksploitasi oleh musuh; dan b. Mengungkapkan pesan kesalahan hanya ke [Penugasa n: personel atau peran yang ditentukan organisasi]. Panduan Tambahan: Organizat ions dengan hati-hati mempertimbangkan structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operation al requirements. Information that could be exploited by adversaries includes, for example, erroneous logon	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	attempts with passwords entered by mistake as the username, mission/business informasi yang dapat diperoleh dari (jika tidak dinyatakan secara eksplisit oleh) informasi yang direkam, dan informasi pribadi seperti nomor rekening, nomor jaminan sosial, dan nomor kartu kredit. Selain itu, pesan kesalahan dapat menyediak an saluran rahasia untuk mengirimkan informasi. Kontrol terkait: AU-2, AU-3, SC-31. Peningkatan Kontrol: Tidak ada. Referensi: Tidak ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-11	Sistem informasi: a. Menghasilkan pesan kesalahan yang memberikan informasi yang diperlukan untuk tindakan korektif tanpa mengungkapkan informasi yang dapat dieksploitasi oleh musuh; dan b. Mengungkapkan pesan kesalahan hanya ke [Penugasan: personel atau peran yang ditentukan organisasi]. Panduan Tambahan: Organizations dengan hati-hati mempertimbangkan structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	attempts with passwords entered by mistake as the username, mission/business informasi yang dapat diperoleh dari (jika tidak dinyatakan secara eksplisit oleh) informasi yang direkam, dan informasi pribadi seperti nomor rekening, nomor jaminan sosial, dan nomor kartu kredit. Selain itu, pesan kesalahan dapat menyediak an saluran rahasia untuk mengirimkan informasi. Kontrol terkait: AU-2, AU-3, SC-31. Peningkatan Kontrol: Tidak ada. Referensi: Tidak ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	dynamodb-resources-protected-by-rencana cadangan	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	ebs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	efs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	rds-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Relational Database Service (Amazon RDS) Anda merupakan AWS bagian dari paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-16	Sistem informasi mengimplementasikan [Assignment: organization-defined security safeguards] untuk melindungi memorinya dari eksekusi kode yang tidak sah. Panduan Tambahan: Beberapa musuh meluncurkan serangan dengan maksud mengeksekusi kode di wilayah memori yang tidak dapat dieksekusi atau di lokasi memori yang dilarang. Pengamanan keamanan yang digunakan untuk melindungi memori termasuk, misalnya, pencegahan eksekusi data dan pengacakan tata letak ruang alamat. Perlindungan pencegahan eksekusi data dapat diberlakukan dengan perangkat keras atau diberlakukan perangkat lunak dengan perangkat keras yang memberikan kekuatan	ecs-task-definition-memory-batas-keras	Membatasi memori maksimum yang tersedia untuk penampung Amazon Elastic Container Service (ECS) memastikan bahwa penggunaan sumber daya Anda tidak dapat disalahgunakan jika terjadi akses berbahaya ke kontainer Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mekanisme yang lebih besar. Kontrol terkait: AC-25, SC-3. Peningkatan Kontrol: Tidak ada. Referensi: Tidak ada.		

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk FedRAMP (Sedang).

Praktik Terbaik Operasional untuk FedRAMP (Bagian Tinggi 1)

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara Federal Risk and Authorization Management Program (FedRAMP) dan aturan Config terkelola. AWS Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau beberapa kontrol FedRAMP. Kontrol FedRAMP dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (2)	Sistem informasi menerapkan mekanisme kriptografi untuk melindungi kerahasiaan dan integritas sesi akses jarak jauh.	alb-http-to-https-pemeriksaan-pengalihan	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
AC-17 (2)	Sistem informasi menerapkan mekanisme kriptografi untuk melindungi kerahasiaan dan integritas sesi akses jarak jauh.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (2)	Sistem informasi menerapkan mekanisme kriptografi untuk melindungi kerahasiaan dan integritas sesi akses jarak jauh.	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (2)	Sistem informasi menerapkan mekanisme kriptografi untuk melindungi kerahasiaan dan integritas sesi akses jarak jauh.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
AC-17 (2)	Sistem informasi menerapkan mekanisme kriptografi untuk melindungi kerahasiaan dan integritas sesi akses jarak jauh.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (2)	Sistem informasi menerapkan mekanisme kriptografi untuk melindungi kerahasiaan dan integritas sesi akses jarak jauh.	elb-acm-certificate-required	MENGISI INI
AC-17 (2)	Sistem informasi menerapkan mekanisme kriptografi untuk melindungi kerahasiaan dan integritas sesi akses jarak jauh.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sesuai kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsageUsia (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna IAM adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebagai gantinya, buat dan gunakan AWS akun berbasis peran untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna IAM. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna IAM.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna IAM, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (12) (a)	Organisasi: a. Memantau akun sistem informasi untuk [Penugasan: penggunaan atipikal yang ditentukan organisasi].	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (12) (a)	Organisasi: a. Memantau akun sistem informasi untuk [Penugasan: penggunaan atipikal yang ditentukan organisasi].	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (3)	Sistem informasi secara otomatis menonaktifkan akun yang tidak aktif setelah 90 hari untuk akun pengguna.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (3)	Sistem informasi secara otomatis menonaktifkan akun yang tidak aktif setelah 90 hari untuk akun pengguna.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikas i, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisas i].	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikasi, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisasi].	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikasi, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisasi].	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan rincian aktivitas panggilan API dalam AWS akun Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikasi, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisasi].	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan AWS akun yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikasi, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisasi].	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikasi, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisasi].	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikasi, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisasi].	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikasi, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisasi].	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDbEncrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikasi, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisasi].	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikasi, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisasi].	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (f)	Organisasi: f. Membuat, mengaktifkan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisasi].	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (f)	Organisasi: f. Membuat, mengaktif kan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisas i].	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifik asi berdasark an kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkin kan Anda untuk mengatur secara opsional RequireUp percaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (f)	Organisasi: f. Membuat, mengaktif kan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisas i].	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebagai gantinya, buat dan gunakan AWS akun berbasis peran untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (f)	Organisasi: f. Membuat, mengaktif kan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisas i].	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
AC-2 (f)	Organisasi: f. Membuat, mengaktif kan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisas i].	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (f)	Organisasi: f. Membuat, mengaktifkan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisasi].	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (f)	Organisasi: f. Membuat, mengaktif kan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisas i].	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastika n kunci akses IAM diputar sesuai kebijakan organisas i. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurang i dampak bisnis jika kunci dikompromikan. Aturan ini memerluka n nilai rotasi kunci akses (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (f)	Organisasi: f. Membuat, mengaktifkan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisasi].	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna IAM adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (f)	Organisasi: f. Membuat, mengaktif kan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisas i].	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastika n otentikasi multi-fak tor (MFA) diaktifka n untuk semua pengguna IAM. MFA menambahk an lapisan perlindun gan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna IAM.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (f)	Organisasi: f. Membuat, mengaktif kan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisas i].	iam-user-no-policies-periksa	Aturan ini memastika n kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapka n hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (f)	Organisasi: f. Membuat, mengaktif kan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisas i].	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna IAM, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (f)	Organisasi: f. Membuat, mengaktifkan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisasi].	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan AWS akun yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan rincian aktivitas panggilan API dalam AWS akun Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatata n AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-user-group-mem bership-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna IAM adalah anggota setidaknya satu grup. Mengizink an pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifik asi berdasark an kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkin kan Anda untuk mengatur secara opsional RequireUp percaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastika n kunci akses IAM diputar sesuai kebijakan organisas i. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurang i dampak bisnis jika kunci dikompromikan. Aturan ini memerluka n nilai rotasi kunci akses (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebagai gantinya, buat dan gunakan AWS akun berbasis peran untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna IAM. Menempatkan pengguna IAM dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-user-no-policies-periksa	Aturan ini memastika n kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapka n hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastika n otentikasi multi-fak tor (MFA) diaktifka n untuk semua pengguna IAM. MFA menambahk an lapisan perlindun gan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna IAM.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-user-unused-cr edentials-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCreden tialUsage Usia (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna IAM, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	ec2- instance-profile-a ttached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirk an profil instans ke instans Anda dapat membantu pengelola an hak istimewa dan izin paling sedikit.
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-policy-no-stat ements-with-full-a ccess	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna IAM adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebagai gantinya, buat dan gunakan AWS akun berbasis peran untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna IAM. Menempatkan pengguna IAM dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSear ch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerluka n gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	lambda-function-pu blic-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotens i menyebabkan degradasi ketersedi aan sumber daya.
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	sagemaker-notebook -no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/ 0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	acm-certificate-ex piration-check	Pastikan integritas jaringan dilindungi dengan memastika n sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExp iration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSear ch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerluka n gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-5c	Organisasi: c. Mendefinisikan otorisasi akses sistem informasi untuk mendukung pemisahan tugas.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna IAM. Menempatkan pengguna IAM dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-5c	Organisasi: c. Mendefinisikan otorisasi akses sistem informasi untuk mendukung pemisahan tugas.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-5c	Organisasi: c. Mendefinisikan otorisasi akses sistem informasi untuk mendukung pemisahan tugas.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.
AC-5c	Organisasi: c. Mendefinisikan otorisasi akses sistem informasi untuk mendukung pemisahan tugas.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-5c	Organisasi: c. Mendefinisikan otorisasi akses sistem informasi untuk mendukung pemisahan tugas.	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-5c	Organisasi: c. Mendefinisikan otorisasi akses sistem informasi untuk mendukung pemisahan tugas.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-5c	Organisasi: c. Mendefinisikan otorisasi akses sistem informasi untuk mendukung pemisahan tugas.	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
AC-5c	Organisasi: c. Mendefinisikan otorisasi akses sistem informasi untuk mendukung pemisahan tugas.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-5c	Organisasi: c. Mendefinisikan otorisasi akses sistem informasi untuk mendukung pemisahan tugas.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-5c	Organisasi: c. Mendefinisikan otorisasi akses sistem informasi untuk mendukung pemisahan tugas.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebagai gantinya, buat dan gunakan AWS akun berbasis peran untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-5c	Organisasi: c. Mendefinisikan otorisasi akses sistem informasi untuk mendukung pemisahan tugas.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna IAM adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-5c	Organisasi: c. Mendefinisikan otorisasi akses sistem informasi untuk mendukung pemisahan tugas.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild . Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna IAM. Menempatkan pengguna IAM dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebagai gantinya, buat dan gunakan AWS akun berbasis peran untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna IAM adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
AC-6 (2)	Sistem informasi memerlukan penggunaan akun yang tidak memiliki hak istimewa saat mengakses fungsi nonsecurity membatasi eksposur saat beroperasi dari dalam akun atau peran istimewa	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (2)	Sistem informasi memerlukan penggunaan akun yang tidak memiliki hak istimewa saat mengakses fungsi nonsecurity membatasi eksposur saat beroperasi dari dalam akun atau peran istimewa	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (2)	Sistem informasi memerlukan penggunaan akun yang tidak memiliki hak istimewa saat mengakses fungsi nonsecurity membatasi eksposur saat beroperasi dari dalam akun atau peran istimewa	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebagai gantinya, buat dan gunakan AWS akun berbasis peran untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.
AC-6 (9)	Sistem informasi mencatat pelaksana an fungsi istimewa.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan rincian aktivitas panggilan API dalam AWS akun Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (9)	Sistem informasi mencatat pelaksana an fungsi istimewa.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan AWS akun yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (9)	Sistem informasi mencatat pelaksana an fungsi istimewa.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (9)	Sistem informasi mencatat pelaksana an fungsi istimewa.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.
AC-6 (9)	Sistem informasi mencatat pelaksana an fungsi istimewa.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteks i aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (9)	Sistem informasi mencatat pelaksana an fungsi istimewa.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (9)	Sistem informasi mencatat pelaksana an fungsi istimewa.	redshift-cluster-c onfiguration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastika n bahwa konfigura si yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberika n informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapka n untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (9)	Sistem informasi mencatat pelaksana an fungsi istimewa.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediak an metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinc i untuk permintaa n yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (10)	Sistem informasi mencegah pengguna yang tidak memiliki hak istimewa untuk menjalankan fungsi istimewa untuk menyertakan menonaktifkan, menghindari, atau mengubah pengamanan keamanan/penanggulangan yang diterapkan.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebagai gantinya, buat dan gunakan AWS akun berbasis peran untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (10)	Sistem informasi mencegah pengguna yang tidak memiliki hak istimewa untuk menjalankan fungsi istimewa untuk menyertakan menonaktifkan, menghindari, atau mengubah pengamanan keamanan/penanggulangan yang diterapkan.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (10)	Sistem informasi mencegah pengguna yang tidak memiliki hak istimewa untuk menjalankan fungsi istimewa untuk menyertakan menonaktifkan, menghindari, atau mengubah pengamanan keamanan/penanggulangan yang diterapkan.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
AU-11	Organisasi menyimpan catatan audit setidaknya selama 90 hari untuk memberikan dukungan untuk after-the-fact investigasi insiden keamanan dan untuk memenuhi persyaratan penyimpanan informasi peraturan dan organisasi.	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di semua sistem informasi dan komponen jaringan di mana kemampuan audit disebarkan/tersedia c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di semua sistem informasi dan komponen jaringan di mana kemampuan audit disebarkan/tersedia c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan rincian aktivitas panggilan API dalam AWS akun Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di semua sistem informasi dan komponen jaringan di mana kemampuan audit disebarkan/tersedia c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di semua sistem informasi dan komponen jaringan di mana kemampuan audit disebarkan/tersedia c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di semua sistem informasi dan komponen jaringan di mana kemampuan audit disebarkan/tersedia c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan AWS akun yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di semua sistem informasi dan komponen jaringan di mana kemampuan audit disebarkan/tersedia c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di semua sistem informasi dan komponen jaringan di mana kemampuan audit disebarkan/tersedia c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di semua sistem informasi dan komponen jaringan di mana kemampuan audit disebarkan/tersedia c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di semua sistem informasi dan komponen jaringan di mana kemampuan audit disebarkan/tersedia c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di semua sistem informasi dan komponen jaringan di mana kemampuan audit disebarkan/tersedia c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di semua sistem informasi dan komponen jaringan di mana kemampuan audit disebarkan/tersedia c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa berikut: Kejadian login akun yang berhasil dan tidak berhasil, peristiwa manajemen akun, akses objek, perubahan kebijakan , fungsi hak istimewa, pelacakan proses, dan peristiwa sistem. Untuk aplikasi Web: semua aktivitas administr ator, pemeriksa an otentikasi, pemeriksaan otorisasi , penghapusan data, akses data, perubahan data, dan perubahan izin. d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [subset yang ditentuka n organisasi dari peristiwa yang dapat diaudit yang didefinis ikan dalam AU-2 a untuk diaudit terus	api-gw-execution-l ogging-diaktifkan	Pencatatan API Gateway menampilk an tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	menerus untuk setiap peristiwa yang diidentifikasi].		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa berikut: Kejadian login akun yang berhasil dan tidak berhasil, peristiwa manajemen akun, akses objek, perubahan kebijakan , fungsi hak istimewa, pelacakan proses, dan peristiwa sistem. Untuk aplikasi Web: semua aktivitas administr ator, pemeriksa an otentikasi, pemeriksaan otorisasi , penghapusan data, akses data, perubahan data, dan perubahan izin. d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [subset yang ditentuka n organisasi dari peristiwa yang dapat diaudit yang didefinis ikan dalam AU-2 a untuk diaudit terus	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan rincian aktivitas panggilan API dalam AWS akun Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	menerus untuk setiap peristiwa yang diidentifikasi].		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa berikut: Kejadian login akun yang berhasil dan tidak berhasil, peristiwa manajemen akun, akses objek, perubahan kebijakan , fungsi hak istimewa, pelacakan proses, dan peristiwa sistem. Untuk aplikasi Web: semua aktivitas administr ator, pemeriksa an otentikasi, pemeriksaan otorisasi , penghapusan data, akses data, perubahan data, dan perubahan izin. d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [subset yang ditentuka n organisasi dari peristiwa yang dapat diaudit yang didefinis ikan dalam AU-2 a untuk diaudit terus	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteks i aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	menerus untuk setiap peristiwa yang diidentifikasi].		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa berikut: Kejadian login akun yang berhasil dan tidak berhasil, peristiwa manajemen akun, akses objek, perubahan kebijakan , fungsi hak istimewa, pelacakan proses, dan peristiwa sistem. Untuk aplikasi Web: semua aktivitas administr ator, pemeriksa an otentikasi, pemeriksaan otorisasi , penghapusan data, akses data, perubahan data, dan perubahan izin. d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [subset yang ditentuka n organisasi dari peristiwa yang dapat diaudit yang didefinis ikan dalam AU-2 a untuk diaudit terus	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan AWS akun yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	menerus untuk setiap peristiwa yang diidentifikasi].		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa berikut: Kejadian login akun yang berhasil dan tidak berhasil, peristiwa manajemen akun, akses objek, perubahan kebijakan , fungsi hak istimewa, pelacakan proses, dan peristiwa sistem. Untuk aplikasi Web: semua aktivitas administr ator, pemeriksa an otentikasi, pemeriksaan otorisasi , penghapusan data, akses data, perubahan data, dan perubahan izin. d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [subset yang ditentuka n organisasi dari peristiwa yang dapat diaudit yang didefinis ikan dalam AU-2 a untuk diaudit terus	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	menerus untuk setiap peristiwa yang diidentifikasi].		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa berikut: Kejadian login akun yang berhasil dan tidak berhasil, peristiwa manajemen akun, akses objek, perubahan kebijakan , fungsi hak istimewa, pelacakan proses, dan peristiwa sistem. Untuk aplikasi Web: semua aktivitas administr ator, pemeriksa an otentikasi, pemeriksaan otorisasi , penghapusan data, akses data, perubahan data, dan perubahan izin. d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [subset yang ditentuka n organisasi dari peristiwa yang dapat diaudit yang didefinis ikan dalam AU-2 a untuk diaudit terus	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	menerus untuk setiap peristiwa yang diidentifikasi].		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa berikut: Kejadian login akun yang berhasil dan tidak berhasil, peristiwa manajemen akun, akses objek, perubahan kebijakan, fungsi hak istimewa, pelacakan proses, dan peristiwa sistem. Untuk aplikasi Web: semua aktivitas administrator, pemeriksaan otentikasi, pemeriksaan otorisasi, penghapusan data, akses data, perubahan data, dan perubahan izin. d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [subset yang ditentukan organisasi dari peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a untuk diaudit terus	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	menerus untuk setiap peristiwa yang diidentifikasi].		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa berikut: Kejadian login akun yang berhasil dan tidak berhasil, peristiwa manajemen akun, akses objek, perubahan kebijakan , fungsi hak istimewa, pelacakan proses, dan peristiwa sistem. Untuk aplikasi Web: semua aktivitas administr ator, pemeriksa an otentikasi, pemeriksaan otorisasi , penghapusan data, akses data, perubahan data, dan perubahan izin. d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [subset yang ditentuka n organisasi dari peristiwa yang dapat diaudit yang didefinis ikan dalam AU-2 a untuk diaudit terus	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	menerus untuk setiap peristiwa yang diidentifikasi].		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa berikut: Kejadian login akun yang berhasil dan tidak berhasil, peristiwa manajemen akun, akses objek, perubahan kebijakan , fungsi hak istimewa, pelacakan proses, dan peristiwa sistem. Untuk aplikasi Web: semua aktivitas administr ator, pemeriksa an otentikasi, pemeriksaan otorisasi , penghapusan data, akses data, perubahan data, dan perubahan izin. d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [subset yang ditentuka n organisasi dari peristiwa yang dapat diaudit yang didefinis ikan dalam AU-2 a untuk diaudit terus	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	menerus untuk setiap peristiwa yang diidentifikasi].		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa berikut: Kejadian login akun yang berhasil dan tidak berhasil, peristiwa manajemen akun, akses objek, perubahan kebijakan , fungsi hak istimewa, pelacakan proses, dan peristiwa sistem. Untuk aplikasi Web: semua aktivitas administr ator, pemeriksa an otentikasi, pemeriksaan otorisasi , penghapusan data, akses data, perubahan data, dan perubahan izin. d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [subset yang ditentuka n organisasi dari peristiwa yang dapat diaudit yang didefinis ikan dalam AU-2 a untuk diaudit terus	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatata n AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	menerus untuk setiap peristiwa yang diidentifikasi].		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa berikut: Kejadian login akun yang berhasil dan tidak berhasil, peristiwa manajemen akun, akses objek, perubahan kebijakan, fungsi hak istimewa, pelacakan proses, dan peristiwa sistem. Untuk aplikasi Web: semua aktivitas administrator, pemeriksaan otentikasi, pemeriksaan otorisasi, penghapusan data, akses data, perubahan data, dan perubahan izin. d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [subset yang ditentukan organisasi dari peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a untuk diaudit terus	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	menerus untuk setiap peristiwa yang diidentifikasi].		
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan rincian aktivitas panggilan API dalam AWS akun Anda.
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan AWS akun yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan rincian aktivitas panggilan API dalam AWS akun Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisas i menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisas i untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisas i menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan AWS akun yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatata n AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	cw-loggroup-retent ion-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonst ruksi dan mengident ifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (3)	Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (3)	Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (3)	Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
AU-6 (3)	Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (3)	Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan rincian aktivitas panggilan API dalam AWS akun Anda.
AU-6 (3)	Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan AWS akun yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (3)	Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
AU-6 (3)	Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (3)	Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (3)	Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (3)	Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (3)	Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-7	Sistem informasi menyediakan dan mengimplementasikan pengurangan catatan audit dan kemampuan pembuatan laporan yang: a. Mendukung peninjauan catatan audit sesuai permintaan, analisis, dan persyaratan pelaporan serta after-the-fact investigasi insiden; dan b. Tidak mengubah konten asli atau urutan waktu catatan audit.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan rincian aktivitas panggilan API dalam AWS akun Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-7	Sistem informasi menyediakan dan mengimplementasikan pengurangan catatan audit dan kemampuan pembuatan laporan yang: a. Mendukung peninjauan catatan audit sesuai permintaan, analisis, dan persyaratan pelaporan serta after-the-fact investigasi insiden; dan b. Tidak mengubah konten asli atau urutan waktu catatan audit.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-7 (1)	Sistem informasi menyediakan kemampuan untuk memproses catatan audit untuk peristiwa yang menarik berdasarkan [Penugasan: bidang audit yang ditentukan organisasi dalam catatan audit].	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-7 (1)	Sistem informasi menyediakan kemampuan untuk memproses catatan audit untuk peristiwa yang menarik berdasarkan [Penugasan: bidang audit yang ditentuka n organisasi dalam catatan audit].	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan rincian aktivitas panggilan API dalam AWS akun Anda.
AU-9	Sistem informasi melindungi informasi audit dan alat audit dari akses, modifikas i, dan penghapusan yang tidak sah.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrai l jejak Anda.
AU-9	Sistem informasi melindungi informasi audit dan alat audit dari akses, modifikas i, dan penghapusan yang tidak sah.	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-9	Sistem informasi melindungi informasi audit dan alat audit dari akses, modifikasi, dan penghapusan yang tidak sah.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-9 (2)	Sistem informasi mencadangkan catatan audit setidaknya setiap minggu ke sistem atau komponen sistem yang berbeda secara fisik dari sistem atau komponen yang diaudit.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-9 (2)	Sistem informasi mencadangkan catatan audit setidaknya setiap minggu ke sistem atau komponen sistem yang berbeda secara fisik dari sistem atau komponen yang diaudit.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Sistem informasi menyediakan kemampuan pembuatan catatan audit untuk jenis acara yang mampu diaudit oleh sistem seperti yang didefinisikan dalam AU-2a pada [Penugasan: komponen sistem yang ditentukan organisasi]; b. Izinkan [Penugasan: personel atau peran yang ditentukan organisasi] untuk memilih jenis acara yang akan dicatat oleh komponen tertentu dari sistem; dan c. Hasilkan catatan audit untuk jenis peristiwa yang ditentukan dalam AU-2c yang mencakup konten catatan audit yang ditentukan dalam AU-3.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Sistem informasi menyediakan kemampuan pembuatan catatan audit untuk jenis acara yang mampu diaudit oleh sistem seperti yang didefinisikan dalam AU-2a pada [Penugasan: komponen sistem yang ditentukan organisasi]; b. Izinkan [Penugasan: personel atau peran yang ditentukan organisasi] untuk memilih jenis acara yang akan dicatat oleh komponen tertentu dari sistem; dan c. Hasilkan catatan audit untuk jenis peristiwa yang ditentukan dalam AU-2c yang mencakup konten catatan audit yang ditentukan dalam AU-3.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Sistem informasi menyediakan kemampuan pembuatan catatan audit untuk jenis acara yang mampu diaudit oleh sistem seperti yang didefinis ikan dalam AU-2a pada [Penugasan: komponen sistem yang ditentukan organisasi]; b. Izinkan [Penugasan: personel atau peran yang ditentukan organisas i] untuk memilih jenis acara yang akan dicatat oleh komponen tertentu dari sistem; dan c. Hasilkan catatan audit untuk jenis peristiwa yang ditentukan dalam AU-2c yang mencakup konten catatan audit yang ditentukan dalam AU-3.	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatata n AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Sistem informasi menyediakan kemampuan pembuatan catatan audit untuk jenis acara yang mampu diaudit oleh sistem seperti yang didefinisikan dalam AU-2a pada [Penugasan: komponen sistem yang ditentukan organisasi]; b. Izinkan [Penugasan: personel atau peran yang ditentukan organisasi] untuk memilih jenis acara yang akan dicatat oleh komponen tertentu dari sistem; dan c. Hasilkan catatan audit untuk jenis peristiwa yang ditentukan dalam AU-2c yang mencakup konten catatan audit yang ditentukan dalam AU-3.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Sistem informasi menyediakan kemampuan pembuatan catatan audit untuk jenis acara yang mampu diaudit oleh sistem seperti yang didefinis ikan dalam AU-2a pada [Penugasan: komponen sistem yang ditentukan organisasi]; b. Izinkan [Penugasan: personel atau peran yang ditentukan organisas i] untuk memilih jenis acara yang akan dicatat oleh komponen tertentu dari sistem; dan c. Hasilkan catatan audit untuk jenis peristiwa yang ditentukan dalam AU-2c yang mencakup konten catatan audit yang ditentukan dalam AU-3.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan rincian aktivitas panggilan API dalam AWS akun Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Sistem informasi menyediakan kemampuan pembuatan catatan audit untuk jenis acara yang mampu diaudit oleh sistem seperti yang didefinis ikan dalam AU-2a pada [Penugasan: komponen sistem yang ditentukan organisasi]; b. Izinkan [Penugasan: personel atau peran yang ditentukan organisas i] untuk memilih jenis acara yang akan dicatat oleh komponen tertentu dari sistem; dan c. Hasilkan catatan audit untuk jenis peristiwa yang ditentukan dalam AU-2c yang mencakup konten catatan audit yang ditentukan dalam AU-3.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan AWS akun yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Sistem informasi menyediakan kemampuan pembuatan catatan audit untuk jenis acara yang mampu diaudit oleh sistem seperti yang didefinisikan dalam AU-2a pada [Penugasan: komponen sistem yang ditentukan organisasi]; b. Izinkan [Penugasan: personel atau peran yang ditentukan organisasi] untuk memilih jenis acara yang akan dicatat oleh komponen tertentu dari sistem; dan c. Hasilkan catatan audit untuk jenis peristiwa yang ditentukan dalam AU-2c yang mencakup konten catatan audit yang ditentukan dalam AU-3.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Sistem informasi menyediakan kemampuan pembuatan catatan audit untuk jenis acara yang mampu diaudit oleh sistem seperti yang didefinisikan dalam AU-2a pada [Penugasan: komponen sistem yang ditentukan organisasi]; b. Izinkan [Penugasan: personel atau peran yang ditentukan organisasi] untuk memilih jenis acara yang akan dicatat oleh komponen tertentu dari sistem; dan c. Hasilkan catatan audit untuk jenis peristiwa yang ditentukan dalam AU-2c yang mencakup konten catatan audit yang ditentukan dalam AU-3.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Sistem informasi menyediakan kemampuan pembuatan catatan audit untuk jenis acara yang mampu diaudit oleh sistem seperti yang didefinis ikan dalam AU-2a pada [Penugasan: komponen sistem yang ditentukan organisasi]; b. Izinkan [Penugasan: personel atau peran yang ditentukan organisas i] untuk memilih jenis acara yang akan dicatat oleh komponen tertentu dari sistem; dan c. Hasilkan catatan audit untuk jenis peristiwa yang ditentukan dalam AU-2c yang mencakup konten catatan audit yang ditentukan dalam AU-3.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Sistem informasi menyediakan kemampuan pembuatan catatan audit untuk jenis acara yang mampu diaudit oleh sistem seperti yang didefinisikan dalam AU-2a pada [Penugasan: komponen sistem yang ditentukan organisasi]; b. Izinkan [Penugasan: personel atau peran yang ditentukan organisasi] untuk memilih jenis acara yang akan dicatat oleh komponen tertentu dari sistem; dan c. Hasilkan catatan audit untuk jenis peristiwa yang ditentukan dalam AU-2c yang mencakup konten catatan audit yang ditentukan dalam AU-3.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Sistem informasi menyediakan kemampuan pembuatan catatan audit untuk jenis acara yang mampu diaudit oleh sistem seperti yang didefinisikan dalam AU-2a pada [Penugasan: komponen sistem yang ditentukan organisasi]; b. Izinkan [Penugasan: personel atau peran yang ditentukan organisasi] untuk memilih jenis acara yang akan dicatat oleh komponen tertentu dari sistem; dan c. Hasilkan catatan audit untuk jenis peristiwa yang ditentukan dalam AU-2c yang mencakup konten catatan audit yang ditentukan dalam AU-3.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Sistem informasi menyediakan kemampuan pembuatan catatan audit untuk jenis acara yang mampu diaudit oleh sistem seperti yang didefinis ikan dalam AU-2a pada [Penugasan: komponen sistem yang ditentukan organisasi]; b. Izinkan [Penugasan: personel atau peran yang ditentukan organisas i] untuk memilih jenis acara yang akan dicatat oleh komponen tertentu dari sistem; dan c. Hasilkan catatan audit untuk jenis peristiwa yang ditentukan dalam AU-2c yang mencakup konten catatan audit yang ditentukan dalam AU-3.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantauan berkelanjutan dan menerapkan program pemantauan berkelanjutan yang meliputi: a. Pembentukan [Penugasan: metrik yang ditentukan organisasi] untuk dipantau; b. Pembentukan [Penugasan: frekuensi yang ditentukan organisasi] untuk pemantauan dan [Penugasan: frekuensi yang ditentukan organisasi] untuk penilaian yang mendukung pemantauan tersebut	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantaua n berkelanjutan dan menerapkan program pemantauan berkelanj utan yang meliputi: a. Pembentuk an [Penugasa n: metrik yang ditentukan organisas i] untuk dipantau; b. Pembentuk an [Penugasan: frekuensi yang ditentukan organisas i] untuk pemantaua n dan [Penugasa n: frekuensi yang ditentukan organisas i] untuk penilaian yang mendukung pemantauan tersebut	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantauan berkelanjutan dan menerapkan program pemantauan berkelanjutan yang meliputi: a. Pembentukan [Penugasan: metrik yang ditentukan organisasi] untuk dipantau; b. Pembentukan [Penugasan: frekuensi yang ditentukan organisasi] untuk pemantauan dan [Penugasan: frekuensi yang ditentukan organisasi] untuk penilaian yang mendukung pemantauan tersebut	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantaua n berkelanjutan dan menerapkan program pemantauan berkelanj utan yang meliputi: a. Pembentuk an [Penugasa n: metrik yang ditentukan organisas i] untuk dipantau; b. Pembentuk an [Penugasan: frekuensi yang ditentukan organisas i] untuk pemantaua n dan [Penugasa n: frekuensi yang ditentukan organisas i] untuk penilaian yang mendukung pemantauan tersebut	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantaua n berkelanjutan dan menerapkan program pemantauan berkelanj utan yang meliputi: a. Pembentuk an [Penugasa n: metrik yang ditentukan organisas i] untuk dipantau; b. Pembentuk an [Penugasan: frekuensi yang ditentukan organisas i] untuk pemantaua n dan [Penugasa n: frekuensi yang ditentukan organisas i] untuk penilaian yang mendukung pemantauan tersebut	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantauan berkelanjutan dan menerapkan program pemantauan berkelanjutan yang meliputi: a. Pembentukan [Penugasan: metrik yang ditentukan organisasi] untuk dipantau; b. Pembentukan [Penugasan: frekuensi yang ditentukan organisasi] untuk pemantauan dan [Penugasan: frekuensi yang ditentukan organisasi] untuk penilaian yang mendukung pemantauan tersebut	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantauan berkelanjutan dan menerapkan program pemantauan berkelanjutan yang meliputi: a. Pembentukan [Penugasan: metrik yang ditentukan organisasi] untuk dipantau; b. Pembentukan [Penugasan: frekuensi yang ditentukan organisasi] untuk pemantauan dan [Penugasan: frekuensi yang ditentukan organisasi] untuk penilaian yang mendukung pemantauan tersebut	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantaua n berkelanjutan dan menerapkan program pemantauan berkelanj utan yang meliputi: a. Pembentuk an [Penugasa n: metrik yang ditentukan organisas i] untuk dipantau; b. Pembentuk an [Penugasan: frekuensi yang ditentukan organisas i] untuk pemantaua n dan [Penugasa n: frekuensi yang ditentukan organisas i] untuk penilaian yang mendukung pemantauan tersebut	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan AWS akun yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantaua n berkelanjutan dan menerapkan program pemantauan berkelanj utan yang meliputi: a. Pembentuk an [Penugasa n: metrik yang ditentukan organisas i] untuk dipantau; b. Pembentuk an [Penugasan: frekuensi yang ditentukan organisas i] untuk pemantaua n dan [Penugasa n: frekuensi yang ditentukan organisas i] untuk penilaian yang mendukung pemantauan tersebut	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteks i aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantauan berkelanjutan dan menerapkan program pemantauan berkelanjutan yang meliputi: a. Pembentukan [Penugasan: metrik yang ditentukan organisasi] untuk dipantau; b. Pembentukan [Penugasan: frekuensi yang ditentukan organisasi] untuk pemantauan dan [Penugasan: frekuensi yang ditentukan organisasi] untuk penilaian yang mendukung pemantauan tersebut	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantauan berkelanjutan dan menerapkan program pemantauan berkelanjutan yang meliputi: a. Pembentukan [Penugasan: metrik yang ditentukan organisasi] untuk dipantau; b. Pembentukan [Penugasan: frekuensi yang ditentukan organisasi] untuk pemantauan dan [Penugasan: frekuensi yang ditentukan organisasi] untuk penilaian yang mendukung pemantauan tersebut	lambda-concurrency-check	Aturan ini memastikan bahwa batas tinggi dan rendah konkurensi fungsi Lambda ditetapkan. Ini dapat membantu dalam mendasarkan jumlah permintaan yang dilayani oleh fungsi Anda pada waktu tertentu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantaua n berkelanjutan dan menerapkan program pemantauan berkelanj utan yang meliputi: a. Pembentuk an [Penugasa n: metrik yang ditentukan organisas i] untuk dipantau; b. Pembentuk an [Penugasan: frekuensi yang ditentukan organisas i] untuk pemantaua n dan [Penugasa n: frekuensi yang ditentukan organisas i] untuk penilaian yang mendukung pemantauan tersebut	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantaua n berkelanjutan dan menerapkan program pemantauan berkelanj utan yang meliputi: a. Pembentuk an [Penugasa n: metrik yang ditentukan organisas i] untuk dipantau; b. Pembentuk an [Penugasan: frekuensi yang ditentukan organisas i] untuk pemantaua n dan [Penugasa n: frekuensi yang ditentukan organisas i] untuk penilaian yang mendukung pemantauan tersebut	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantauan berkelanjutan dan menerapkan program pemantauan berkelanjutan yang meliputi: a. Pembentukan [Penugasan: metrik yang ditentukan organisasi] untuk dipantau; b. Pembentukan [Penugasan: frekuensi yang ditentukan organisasi] untuk pemantauan dan [Penugasan: frekuensi yang ditentukan organisasi] untuk penilaian yang mendukung pemantauan tersebut	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigurasi dasar saat ini dari sistem informasi.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	ec2- volume-inuse-check	Aturan ini memastika n bahwa volume Amazon Elastic Block Store yang dilampirk an ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentika n, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigurasi dasar saat ini dari sistem informasi.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigurasi dasar saat ini dari sistem informasi.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigurasi dasar saat ini dari sistem informasi.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigurasi dasar saat ini dari sistem informasi.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	sagemaker-notebook -no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/ 0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurk an ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfig urasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizink an, memblokir, atau menghitung permintaa n web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindung inya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigurasi dasar saat ini dari sistem informasi.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-7 (a)	Organisasi: a. Mengkonfigurasi sistem informasi untuk hanya menyediakan kemampuan penting.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-7 (a)	Organisasi: a. Mengkonfigurasi sistem informasi untuk hanya menyediakan kemampuan penting.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.
CM-7 (a)	Organisasi: a. Mengkonfigurasi sistem informasi untuk hanya menyediakan kemampuan penting.	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-8 (1)	Organisasi memperbarui inventaris komponen sistem informasi sebagai bagian integral dari instalasi komponen, penghapusan, dan pembaruan sistem informasi.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-8 (1)	Organisasi memperbarui inventaris komponen sistem informasi sebagai bagian integral dari instalasi komponen, penghapusan, dan pembaruan sistem informasi.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-8 (3) (a)	Organisasi: a. Menggunakan mekanisme otomatis secara terus menerus, menggunakan mekanisme otomatis dengan penundaan maksimum lima menit dalam deteksi, untuk mendeteks i keberadaan komponen perangkat keras, perangkat lunak, dan firmware yang tidak sah dalam sistem informasi	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-8 (3) (a)	Organisasi: a. Menggunakan mekanisme otomatis secara terus menerus, menggunakan mekanisme otomatis dengan penundaan maksimum lima menit dalam deteksi, untuk mendeteks i keberadaan komponen perangkat keras, perangkat lunak, dan firmware yang tidak sah dalam sistem informasi	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventari s platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-8 (3) (a)	Organisasi: a. Menggunakan mekanisme otomatis secara terus menerus, menggunakan mekanisme otomatis dengan penundaan maksimum lima menit dalam deteksi, untuk mendeteks i keberadaan komponen perangkat keras, perangkat lunak, dan firmware yang tidak sah dalam sistem informasi	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-8 (3) (a)	Organisasi: a. Menggunakan mekanisme otomatis secara terus menerus, menggunakan mekanisme otomatis dengan penundaan maksimum lima menit dalam deteksi, untuk mendeteks i keberadaan komponen perangkat keras, perangkat lunak, dan firmware yang tidak sah dalam sistem informasi	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (1)	Organisasi mengidentifikasi situs penyimpanan alternatif yang cukup terpisah dari situs penyimpanan utama untuk mengurangi kerentanan terhadap ancaman yang sama.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (1)	Organisasi mengidentifikasi situs penyimpanan alternatif yang cukup terpisah dari situs penyimpanan utama untuk mengurangi kerentanan terhadap ancaman yang sama.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (1)	Organisasi mengidentifikasi situs penyimpanan alternatif yang cukup terpisah dari situs penyimpanan utama untuk mengurangi kerentanan terhadap ancaman yang sama.	efs-in-backup-plan	Untuk membantu proses pencadang an data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (1)	Organisasi mengidentifikasi situs penyimpanan alternatif yang cukup terpisah dari situs penyimpanan utama untuk mengurangi kerentanan terhadap ancaman yang sama.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB per node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (1)	Organisasi mengidentifikasi situs penyimpanan alternatif yang cukup terpisah dari situs penyimpanan utama untuk mengurangi kerentanan terhadap ancaman yang sama.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (1)	Organisasi mengidentifikasi situs penyimpanan alternatif yang cukup terpisah dari situs penyimpanan utama untuk mengurangi kerentanan terhadap ancaman yang sama.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (1)	Organisasi mengidentifikasi situs penyimpanan alternatif yang cukup terpisah dari situs penyimpanan utama untuk mengurangi kerentanan terhadap ancaman yang sama.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (1)	Organisasi mengidentifikasi situs penyimpanan alternatif yang cukup terpisah dari situs penyimpanan utama untuk mengurangi kerentanan terhadap ancaman yang sama.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	Sistem informasi a. Melakukan pencadangan informasi tingkat pengguna yang terkandung dalam [Penugasan: komponen sistem yang ditentukan organisasi] [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; b. Melakukan pencadangan informasi tingkat sistem yang terkandung dalam sistem [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumentasi terkait keamanan dan privasi [Penugasa	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	n: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; dan d. Melindungi kerahasiaan, integritas, dan ketersediaan informasi cadangan.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	Sistem informasi a. Melakukan pencadangan informasi tingkat pengguna yang terkandung dalam [Penugasan: komponen sistem yang ditentukan organisasi] [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; b. Melakukan pencadangan informasi tingkat sistem yang terkandung dalam sistem [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumentasi terkait keamanan dan privasi [Penugasa	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	n: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; dan d. Melindungi kerahasiaan, integritas, dan ketersediaan informasi cadangan.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	Sistem informasi a. Melakukan pencadangan informasi tingkat pengguna yang terkandung dalam [Penugasan: komponen sistem yang ditentukan organisasi] [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; b. Melakukan pencadangan informasi tingkat sistem yang terkandung dalam sistem [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumentasi terkait keamanan dan privasi [Penugasa	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	n: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; dan d. Melindungi kerahasiaan, integritas, dan ketersediaan informasi cadangan.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	Sistem informasi a. Melakukan pencadangan informasi tingkat pengguna yang terkandung dalam [Penugasan: komponen sistem yang ditentukan organisasi] [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; b. Melakukan pencadangan informasi tingkat sistem yang terkandung dalam sistem [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumentasi terkait keamanan dan privasi [Penugasa	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB per node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	n: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; dan d. Melindungi kerahasiaan, integritas, dan ketersediaan informasi cadangan.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	Sistem informasi a. Melakukan pencadangan informasi tingkat pengguna yang terkandung dalam [Penugasan: komponen sistem yang ditentukan organisasi] [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; b. Melakukan pencadangan informasi tingkat sistem yang terkandung dalam sistem [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumentasi terkait keamanan dan privasi [Penugasa	s3- version-lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihkan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	n: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; dan d. Melindungi kerahasiaan, integritas, dan ketersediaan informasi cadangan.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	Sistem informasi a. Melakukan pencadangan informasi tingkat pengguna yang terkandung dalam [Penugasan: komponen sistem yang ditentukan organisasi] [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; b. Melakukan pencadangan informasi tingkat sistem yang terkandung dalam sistem [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumentasi terkait keamanan dan privasi [Penugasa	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	n: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; dan d. Melindungi kerahasiaan, integritas, dan ketersediaan informasi cadangan.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	Sistem informasi a. Melakukan pencadangan informasi tingkat pengguna yang terkandung dalam [Penugasan: komponen sistem yang ditentukan organisasi] [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; b. Melakukan pencadangan informasi tingkat sistem yang terkandung dalam sistem [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumentasi terkait keamanan dan privasi [Penugasa	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	n: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; dan d. Melindungi kerahasiaan, integritas, dan ketersediaan informasi cadangan.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	Sistem informasi a. Melakukan pencadangan informasi tingkat pengguna yang terkandung dalam [Penugasan: komponen sistem yang ditentukan organisasi] [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; b. Melakukan pencadangan informasi tingkat sistem yang terkandung dalam sistem [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumentasi terkait keamanan dan privasi [Penugasa	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	n: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; dan d. Melindungi kerahasiaan, integritas, dan ketersediaan informasi cadangan.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	Sistem informasi a. Melakukan pencadangan informasi tingkat pengguna yang terkandung dalam [Penugasan: komponen sistem yang ditentukan organisasi] [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; b. Melakukan pencadangan informasi tingkat sistem yang terkandung dalam sistem [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumentasi terkait keamanan dan privasi [Penugasa	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	n: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; dan d. Melindungi kerahasiaan, integritas, dan ketersediaan informasi cadangan.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	Sistem informasi a. Melakukan pencadangan informasi tingkat pengguna yang terkandung dalam [Penugasan: komponen sistem yang ditentukan organisasi] [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; b. Melakukan pencadangan informasi tingkat sistem yang terkandung dalam sistem [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumentasi terkait keamanan dan privasi [Penugasa	redshift-cluster-maintenancesettings-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	n: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; dan d. Melindungi kerahasiaan, integritas, dan ketersediaan informasi cadangan.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	Sistem informasi a. Melakukan pencadangan informasi tingkat pengguna yang terkandung dalam [Penugasan: komponen sistem yang ditentukan organisasi] [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; b. Melakukan pencadangan informasi tingkat sistem yang terkandung dalam sistem [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumentasi terkait keamanan dan privasi [Penugasa	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	n: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; dan d. Melindungi kerahasiaan, integritas, dan ketersediaan informasi cadangan.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	Sistem informasi a. Melakukan pencadangan informasi tingkat pengguna yang terkandung dalam [Penugasan: komponen sistem yang ditentukan organisasi] [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; b. Melakukan pencadangan informasi tingkat sistem yang terkandung dalam sistem [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumentasi terkait keamanan dan privasi [Penugasa	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	n: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan]; dan d. Melindungi kerahasiaan, integritas, dan ketersediaan informasi cadangan.		
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) menyediakan ketersediaan dan daya tahan yang ditingkatkan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			segera setelah failover selesai.
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB per node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	dynamodb-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	ebs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	efs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	rds-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Relational Database Service (Amazon RDS) Anda merupakan AWS bagian dari paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem informasi (inkremental harian; mingguan penuh).	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem informasi (inkremental harian; mingguan penuh).	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem informasi (inkremental harian; mingguan penuh).	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem informasi (inkremental harian; mingguan penuh).	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem informasi (inkremental harian; mingguan penuh).	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB per node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem informasi (inkremental harian; mingguan penuh).	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem informasi (inkremental harian; mingguan penuh).	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem informasi (inkremental harian; mingguan penuh).	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem informasi (inkremental harian; mingguan penuh).	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem informasi (inkremental harian; mingguan penuh).	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem informasi (inkremental harian; mingguan penuh).	dynamodb-resources-protected-by-rencana cadangan	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem informasi (inkremental harian; mingguan penuh).	ebs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem informasi (inkremental harian; mingguan penuh).	efs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem informasi (inkremental harian; mingguan penuh).	rds-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Relational Database Service (Amazon RDS) Anda merupakan AWS bagian dari paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2	Sistem informasi secara unik mengidentifikasi dan mengotentikasi pengguna organisasi (atau proses yang bertindak atas nama pengguna organisasi).	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2	Sistem informasi secara unik mengidentifikasi dan mengotentikasi pengguna organisasi (atau proses yang bertindak atas nama pengguna organisasi).	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebagai gantinya, buat dan gunakan AWS akun berbasis peran untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2 (1)	(1) Sistem informasi menerapkan otentikasi multifaktor untuk akses jaringan ke akun istimewa.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna IAM. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna IAM.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2 (1)	(1) Sistem informasi menerapkan otentikasi multifaktor untuk akses jaringan ke akun istimewa.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna IAM, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2 (1) (2)	(1) Sistem informasi menerapkan otentikasi multifaktor untuk akses jaringan ke akun istimewa. (2) Sistem informasi menerapkan otentikasi multifaktor untuk akses jaringan ke akun yang tidak memiliki hak istimewa.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna IAM, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2 (1) (2)	(1) Sistem informasi menerapkan otentikasi multifaktor untuk akses jaringan ke akun istimewa. (2) Sistem informasi menerapkan otentikasi multifaktor untuk akses jaringan ke akun yang tidak memiliki hak istimewa.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna IAM. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna IAM.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-5 (1) (a) (d) (e)	Sistem informasi , untuk otentikasi berbasis kata sandi: a. Menegakkan kompleksitas kata sandi minimum [Penugasan: persyaratan yang ditentukan organisasi untuk sensitivitas huruf besar, jumlah karakter, campuran huruf besar, huruf kecil, angka, dan karakter khusus, termasuk persyaratan minimum untuk setiap jenis]; d. Menegakkan batasan masa pakai minimum dan maksimum kata sandi [Penugasan: angka yang ditentukan organisasi untuk minimum seumur hidup, maksimum seumur hidup]; e. Melarang penggunaan kembali kata sandi selama 24 generasi	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-5 (4)	Organisasi menggunakan alat otomatis untuk menentukan apakah autentikator kata sandi cukup kuat untuk memenuhi [Penugasan: persyaratan yang ditentukan organisasi].	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-5 (7)	Organisasi memastikan bahwa autentikator statis yang tidak terenkripsi tidak disematkan dalam aplikasi atau skrip akses atau disimpan pada tombol fungsi.	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild. Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-4 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung proses penanganan insiden.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-4 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung proses penanganan insiden.	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-4 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung proses penanganan insiden.	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-4 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung proses penanganan insiden.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-4 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung proses penanganan insiden.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-6 (1)	Organisasi menggunakan mekanisme otomatis untuk membantu pelaporan insiden keamanan.	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-6 (1)	Organisasi menggunakan mekanisme otomatis untuk membantu pelaporan insiden keamanan.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-6 (1)	Organisasi menggunakan mekanisme otomatis untuk membantu pelaporan insiden keamanan.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-7 (1)	Organisasi ini menggunakan mekanisme otomatis untuk meningkat kan ketersediaan informasi dan dukungan terkait respons insiden.	guardduty-non-arch ived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasark an tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunak an klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSe v (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratk an oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-7 (1)	Organisasi ini menggunakan mekanisme otomatis untuk meningkat kan ketersediaan informasi dan dukungan terkait respons insiden.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-7 (1)	Organisasi ini menggunakan mekanisme otomatis untuk meningkat kan ketersediaan informasi dan dukungan terkait respons insiden.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RA-5	Organisasi: a. Memindai kerentana n dalam sistem informasi dan aplikasi yang dihosting [Penugasan: frekuensi yang ditentukan organisasi diidentif ikasi dan dilaporka n; and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/application s b. Menggunak an alat dan teknik pemindaian kerentana n yang memfasilitasi interoperabilitas antar alat dan mengotoma tiskan bagian dari proses manajemen kerentanan dengan menggunakan standar untuk: 1. Mencacah platform, kelemahan perangkat lunak, dan konfigurasi yang tidak tepat; 2. Memformat daftar periksa dan prosedur pengujian ; dan 3. Mengukur	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dampak kerentana n; c. Menganalisis laporan pemindaia n kerentanan dan hasil dari penilaian kontrol keamanan; d. Memulihkan kerentanan yang sah [Penugasa n: waktu respons yang ditentukan organisasi], sesuai dengan penilaian risiko organisasi; dan e. Membagika n informasi yang diperoleh dari proses pemindaian kerentana n dan penilaian kontrol keamanan dengan [Penugasa n: personel atau peran yang ditentuka n organisasi] untuk membantu menghilan gkan kerentanan serupa dalam sistem informasi lain (yaitu, kelemahan atau kekurangan sistemik).		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RA-5	Organisasi: a. Memindai kerentana n dalam sistem informasi dan aplikasi yang dihosting setiap bulan [operasi system/infrastruct ure; monthly web applications and databases] and when new vulnerabi lities potentially affecting the system/ applications diidentif ikasi dan dilaporka n; b. Menggunak an alat dan teknik pemindaian kerentana n yang memfasilitasi interoperabilitas antar alat dan mengotoma tiskan bagian dari proses manajemen kerentanan dengan menggunakan standar untuk: 1. Mencacah platform, kelemahan perangkat lunak, dan konfigurasi yang tidak tepat; 2. Memformat daftar periksa dan prosedur pengujian ; dan 3. Mengukur dampak kerentana	guardduty-non-arch ived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasark an tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunak an klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSe v (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratk an oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	n; c. Menganalisis laporan pemindaian kerentanan dan hasil dari penilaian kontrol keamanan; d. Memperbaiki kerentanan yang sah: kerentanan berisiko tinggi dikurangi dalam waktu tiga puluh (30) hari sejak tanggal penemuan; kerentanan risiko sedang dikurangi dalam sembilan puluh (90) hari sejak tanggal penemuan; kerentanan risiko rendah dikurangi dalam seratus delapan puluh (180) hari sejak tanggal penemuan, sesuai dengan penilaian risiko organisasi; dan e. Membagikan informasi yang diperoleh dari proses pemindaian kerentanan dan penilaian kontrol keamanan dengan [Penugasan: personel atau peran yang ditentukan organisasi] untuk		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	membantu menghilangkan kerentanan serupa dalam sistem informasi lain (yaitu, kelemahan atau kekurangan sistemik).		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-10	Organisasi membutuhkan pengembang sistem informasi, komponen sistem, atau layanan sistem informasi untuk: a. Melakukan manajemen konfigura si selama pengemban gan sistem, komponen, atau layanan, implement asi, DAN operasi; b. Mendokume ntasikan, mengelola , dan mengontrol integritas perubahan pada [Penugasa n: item konfigura si yang ditentukan organisasi di bawah manajemen konfigura si]; c. Menerapkan hanya perubahan yang disetujui organisasi pada sistem, komponen, atau layanan; d. Mendokumentasikan perubahan yang disetujui pada sistem, komponen, atau layanan dan potensi dampak keamanan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dari perubahan tersebut; dan e. Lacak kelemahan keamanan dan resolusi cacat dalam sistem, komponen, atau layanan dan laporkan temuan ke [Penugasan: personel yang ditentukan organisasi].		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-10	Organisasi membutuhkan pengembang sistem informasi, komponen sistem, atau layanan sistem informasi untuk: a. Melakukan manajemen konfigurasi selama pengembangan sistem, komponen, atau layanan, implementasi, DAN operasi; b. Mendokumentasikan, mengelola, dan mengontrol integritas perubahan pada [Penugasan: item konfigurasi yang ditentukan organisasi di bawah manajemen konfigurasi]; c. Menerapkan hanya perubahan yang disetujui organisasi pada sistem, komponen, atau layanan; d. Mendokumentasikan perubahan yang disetujui pada sistem, komponen, atau layanan dan potensi dampak keamanan	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan: rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dari perubahan tersebut; dan e. Lacak kelemahan keamanan dan resolusi cacat dalam sistem, komponen, atau layanan dan laporkan temuan ke [Penugasan: personel yang ditentukan organisasi].		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-10	Organisasi membutuhkan pengembang sistem informasi, komponen sistem, atau layanan sistem informasi untuk: a. Melakukan manajemen konfigura si selama pengemban gan sistem, komponen, atau layanan, implement asi, DAN operasi; b. Mendokume ntasikan, mengelola , dan mengontrol integritas perubahan pada [Penugasa n: item konfigura si yang ditentukan organisasi di bawah manajemen konfigura si]; c. Menerapkan hanya perubahan yang disetujui organisasi pada sistem, komponen, atau layanan; d. Mendokumentasikan perubahan yang disetujui pada sistem, komponen, atau layanan dan potensi dampak keamanan	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dari perubahan tersebut; dan e. Lacak kelemahan keamanan dan resolusi cacat dalam sistem, komponen, atau layanan dan laporkan temuan ke [Penugasan: personel yang ditentukan organisasi].		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-10	Organisasi membutuhkan pengembang sistem informasi, komponen sistem, atau layanan sistem informasi untuk: a. Melakukan manajemen konfigura si selama pengemban gan sistem, komponen, atau layanan, implement asi, DAN operasi; b. Mendokume ntasikan, mengelola , dan mengontrol integritas perubahan pada [Penugasa n: item konfigura si yang ditentukan organisasi di bawah manajemen konfigura si]; c. Menerapkan hanya perubahan yang disetujui organisasi pada sistem, komponen, atau layanan; d. Mendokumentasikan perubahan yang disetujui pada sistem, komponen, atau layanan dan potensi dampak keamanan	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dari perubahan tersebut; dan e. Lacak kelemahan keamanan dan resolusi cacat dalam sistem, komponen, atau layanan dan laporkan temuan ke [Penugasan: personel yang ditentukan organisasi].		
SA-3 (a)	Organisasi: a. Mengelola sistem informasi menggunakan [Penugasan: siklus hidup pengembangan sistem yang ditentukan organisasi] yang menggabungkan pertimbangan keamanan informasi.	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild . Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-3 (a)	Organisasi: a. Mengelola sistem informasi menggunakan [Penugasan: siklus hidup pengembangan sistem yang ditentukan organisasi] yang menggabungkan pertimbangan keamanan informasi.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-3 (a)	Organisasi: a. Mengelola sistem informasi menggunakan [Penugasan: siklus hidup pengembangan sistem yang ditentukan organisasi] yang menggabungkan pertimbangan keamanan informasi.	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, nama pengguna, dan kata sandi dalam lingkungan proyek AWS Codebuild. Gunakan OAuth alih-alih token akses pribadi atau nama pengguna dan kata sandi untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.
SC-12	Organisasi menetapkan dan mengelola kunci kriptografi untuk kriptografi yang diperlukan yang digunakan dalam sistem informasi sesuai dengan [Penugasan: persyaratan yang ditentukan organisasi untuk pembuatan kunci, distribusi, penyimpanan, akses, dan penghancuran].	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-12	Organisasi menetapkan dan mengelola kunci kriptografi untuk kriptografi yang diperlukan yang digunakan dalam sistem informasi sesuai dengan [Penugasan: persyaratan yang ditentukan organisasi untuk pembuatan kunci, distribusi, penyimpanan, akses, dan penghancuran].	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-12	Organisasi menetapkan dan mengelola kunci kriptografi untuk kriptografi yang diperlukan yang digunakan dalam sistem informasi sesuai dengan [Penugasan: persyaratan yang ditentukan organisasi untuk pembuatan kunci, distribusi, penyimpanan, akses, dan penghancuran].	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13	Sistem informasi menerapkan kriptografi yang divalidasi FIPS atau disetujui NSA sesuai dengan hukum federal yang berlaku, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar.	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-13	Sistem informasi menerapkan kriptografi yang divalidasi FIPS atau disetujui NSA sesuai dengan hukum federal yang berlaku, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar.	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13	Sistem informasi menerapkan kriptografi yang divalidasi FIPS atau disetujui NSA sesuai dengan hukum federal yang berlaku, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar.	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13	Sistem informasi menerapkan kriptografi yang divalidasi FIPS atau disetujui NSA sesuai dengan hukum federal yang berlaku, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar.	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13	Sistem informasi menerapkan kriptografi yang divalidasi FIPS atau disetujui NSA sesuai dengan hukum federal yang berlaku, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar.	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-13	Sistem informasi menerapkan kriptografi yang divalidasi FIPS atau disetujui NSA sesuai dengan hukum federal yang berlaku, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar.	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-2	Sistem informasi memisahkan fungsionalitas pengguna (termasuk layanan antarmuka pengguna) dari fungsi manajemen sistem informasi.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna IAM. Menempatkan pengguna IAM dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-2	Sistem informasi memisahkan fungsionalitas pengguna (termasuk layanan antarmuka pengguna) dari fungsi manajemen sistem informasi.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-2	Sistem informasi memisahkan fungsionalitas pengguna (termasuk layanan antarmuka pengguna) dari fungsi manajemen sistem informasi.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-2	Sistem informasi memisahkan fungsionalitas pengguna (termasuk layanan antarmuka pengguna) dari fungsi manajemen sistem informasi.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna IAM adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-2	Sistem informasi memisahkan fungsionalitas pengguna (termasuk layanan antarmuka pengguna) dari fungsi manajemen sistem informasi.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-23	Sistem informasi melindungi keaslian sesi komunikasi.	alb-http-to-https-pemeriksaan-pengalihan	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-23	Sistem informasi melindungi keaslian sesi komunikasi.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-23	Sistem informasi melindungi keaslian sesi komunikasi.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
SC-23	Sistem informasi melindungi keaslian sesi komunikasi.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-n ode enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkrip si memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-23	Sistem informasi melindungi keaslian sesi komunikasi.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-23	Sistem informasi melindungi keaslian sesi komunikasi.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-28	Sistem informasi melindungi kerahasiaan DAN integritas [Penugasan: informasi yang ditentukan organisasi saat istirahat].	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan melalui sumber daya sistem bersama.	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan melalui sumber daya sistem bersama.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan melalui sumber daya sistem bersama.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan melalui sumber daya sistem bersama.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan melalui sumber daya sistem bersama.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan melalui sumber daya sistem bersama.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan melalui sumber daya sistem bersama.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan melalui sumber daya sistem bersama.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan melalui sumber daya sistem bersama.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan melalui sumber daya sistem bersama.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan melalui sumber daya sistem bersama.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan melalui sumber daya sistem bersama.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan melalui sumber daya sistem bersama.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan melalui sumber daya sistem bersama.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan melalui sumber daya sistem bersama.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan melalui sumber daya sistem bersama.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan melalui sumber daya sistem bersama.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan melalui sumber daya sistem bersama.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) menyediakan ketersediaan dan daya tahan yang ditingkatkan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			segera setelah failover selesai.
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigurasi ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	alb-http-to-https-pemeriksaan-pengalihan	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8	Sistem informasi melindungi kerahasia an DAN integrita s informasi yang dikirimkan.	alb-http-to-https-pemeriksaan-pengal ihan	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-8	Sistem informasi melindungi kerahasia an DAN integrita s informasi yang dikirimkan.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-n ode enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkrip si memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8	Sistem informasi melindungi kerahasia an DAN integrita s informasi yang dikirimkan.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-8	Sistem informasi melindungi kerahasia an DAN integrita s informasi yang dikirimkan.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8	Sistem informasi melindungi kerahasia an DAN integrita s informasi yang dikirimkan.	s3- bucket-ssl-request s-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-8	Sistem informasi melindungi kerahasia an DAN integrita s informasi yang dikirimkan.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8 (1)	Sistem informasi menerapkan mekanisme kriptografi untuk [Seleksi (satu atau lebih): mencegah pengungkapan informasi yang tidak sah; mendeteksi perubahan informasi] selama transmisi kecuali dilindungi oleh [Penugasan: perlindungan fisik alternatif yang ditentukan organisasi].	alb-http-to-https-pemeriksaan-pengalihan	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-8 (1)	Sistem informasi menerapkan mekanisme kriptografi untuk [Seleksi (satu atau lebih): mencegah pengungkapan informasi yang tidak sah; mendeteksi perubahan informasi] selama transmisi kecuali dilindungi oleh [Penugasan: perlindungan fisik alternatif yang ditentukan organisasi].	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8 (1)	Sistem informasi menerapkan mekanisme kriptografi untuk [Seleksi (satu atau lebih): mencegah pengungkapan informasi yang tidak sah; mendeteksi perubahan informasi] selama transmisi kecuali dilindungi oleh [Penugasan: perlindungan fisik alternatif yang ditentukan organisasi].	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-8 (1)	Sistem informasi menerapkan mekanisme kriptografi untuk [Seleksi (satu atau lebih): mencegah pengungkapan informasi yang tidak sah; mendeteksi perubahan informasi] selama transmisi kecuali dilindungi oleh [Penugasan: perlindungan fisik alternatif yang ditentukan organisasi].	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8 (1)	Sistem informasi menerapkan mekanisme kriptografi untuk [Seleksi (satu atau lebih): mencegah pengungkapan informasi yang tidak sah; mendeteksi perubahan informasi] selama transmisi kecuali dilindungi oleh [Penugasan: perlindungan fisik alternatif yang ditentukan organisasi].	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-8 (1)	Sistem informasi menerapkan mekanisme kriptografi untuk [Seleksi (satu atau lebih): mencegah pengungkapan informasi yang tidak sah; mendeteksi perubahan informasi] selama transmisi kecuali dilindungi oleh [Penugasan: perlindungan fisik alternatif yang ditentukan organisasi].	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB per node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	dynamodb-resources-protected-by-rencana cadangan	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	ebs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	efs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	rds-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Relational Database Service (Amazon RDS) Anda merupakan AWS bagian dari paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2 (2)	Organisasi menggunak an mekanisme otomatis setidakny a setiap bulan untuk menentukan keadaan komponen sistem informasi sehubunga n dengan remediasi cacat.	ec2- -periksa managedinstance-pa tch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2 (2)	Organisasi menggunak an mekanisme otomatis setidakny a setiap bulan untuk menentukan keadaan komponen sistem informasi sehubunga n dengan remediasi cacat.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2 (2)	Organisasi menggunak an mekanisme otomatis setidakny a setiap bulan untuk menentukan keadaan komponen sistem informasi sehubunga n dengan remediasi cacat.	ec2- -periksa managedinstance-as sociation-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventari s platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2 (2)	Organisasi menggunak an mekanisme otomatis setidakny a setiap bulan untuk menentukan keadaan komponen sistem informasi sehubunga n dengan remediasi cacat.	elastic-beanstalk-managed-updates-di aktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (1)	Organisasi menghubungkan dan mengonfigurasi alat deteksi intrusi individu ke dalam sistem deteksi intrusi di seluruh sistem informasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (16)	Organisasi menghubungkan informasi dari alat pemantauan yang digunakan di seluruh sistem informasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (16)	Organisasi menghubungkan informasi dari alat pemantauan yang digunakan di seluruh sistem informasi.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (16)	Organisasi menghubungkan informasi dari alat pemantauan yang digunakan di seluruh sistem informasi.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (16)	Organisasi menghubungkan informasi dari alat pemantauan yang digunakan di seluruh sistem informasi.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (16)	Organisasi menghubungkan informasi dari alat pemantauan yang digunakan di seluruh sistem informasi.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan AWS akun yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (16)	Organisasi menghubungkan informasi dari alat pemantauan yang digunakan di seluruh sistem informasi.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (2)	Organisasi ini menggunakan alat otomatis untuk mendukung analisis peristiwa yang hampir real-time.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (2)	Organisasi ini menggunakan alat otomatis untuk mendukung analisis peristiwa yang hampir real-time.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (2)	Organisasi ini menggunakan alat otomatis untuk mendukung analisis peristiwa yang hampir real-time.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (2)	Organisasi ini menggunakan alat otomatis untuk mendukung analisis peristiwa yang hampir real-time.	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (2)	Organisasi ini menggunakan alat otomatis untuk mendukung analisis peristiwa yang hampir real-time.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (2)	Organisasi ini menggunakan alat otomatis untuk mendukung analisis peristiwa yang hampir real-time.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan AWS akun yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
SI-4 (2)	Organisasi ini menggunakan alat otomatis untuk mendukung analisis peristiwa yang hampir real-time.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (2)	Organisasi ini menggunakan alat otomatis untuk mendukung analisis peristiwa yang hampir real-time.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (4)	Sistem informasi memantau lalu lintas komunikasi masuk dan keluar secara terus menerus untuk aktivitas atau kondisi yang tidak biasa atau tidak sah.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (4)	Sistem informasi memantau lalu lintas komunikasi masuk dan keluar secara terus menerus untuk aktivitas atau kondisi yang tidak biasa atau tidak sah.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (4)	Sistem informasi memantau lalu lintas komunikasi masuk dan keluar secara terus menerus untuk aktivitas atau kondisi yang tidak biasa atau tidak sah.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (4)	Sistem informasi memantau lalu lintas komunikasi masuk dan keluar secara terus menerus untuk aktivitas atau kondisi yang tidak biasa atau tidak sah.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan rincian aktivitas panggilan API dalam AWS akun Anda.
SI-4 (5)	Sistem informasi memperingatkan [Penugasan: personel atau peran yang ditentukan organisasi] ketika indikasi kompromi atau potensi kompromi berikut terjadi: [Penugasan: indikator kompromi yang ditentukan organisasi].	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (5)	Sistem informasi memperingatkan [Penugasan: personel atau peran yang ditentukan organisasi] ketika indikasi kompromi atau potensi kompromi berikut terjadi: [Penugasan: indikator kompromi yang ditentukan organisasi].	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (5)	Sistem informasi memperingatkan [Penugasan: personel atau peran yang ditentukan organisasi] ketika indikasi kompromi atau potensi kompromi berikut terjadi: [Penugasan: indikator kompromi yang ditentukan organisasi].	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (5)	Sistem informasi memperingatkan [Penugasan: personel atau peran yang ditentukan organisasi] ketika indikasi kompromi atau potensi kompromi berikut terjadi: [Penugasan: indikator kompromi yang ditentukan organisasi].	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan rincian aktivitas panggilan API dalam AWS akun Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (a) (b) (c)	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1. Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2. Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c. Menyebarkan perangkat pemantauan: i. secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan (ii) di lokasi ad hoc dalam sistem untuk melacak jenis transaksi	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	tertentu yang menarik bagi organisasi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (a) (b) (c)	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1. Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2. Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c. Menyebarkan perangkat pemantauan: i. secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan (ii) di lokasi ad hoc dalam sistem untuk melacak jenis transaksi	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan: rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	tertentu yang menarik bagi organisasi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (a) (b) (c)	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1. Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2. Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c. Menyebarkan perangkat pemantauan: i. secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan (ii) di lokasi ad hoc dalam sistem untuk melacak jenis transaksi	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	tertentu yang menarik bagi organisasi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (a) (b) (c)	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1. Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2. Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c. Menyebarkan perangkat pemantauan: i. secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan (ii) di lokasi ad hoc dalam sistem untuk melacak jenis transaksi	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	tertentu yang menarik bagi organisasi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (a) (b) (c)	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1. Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2. Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c. Menyebarkan perangkat pemantauan: i. secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan (ii) di lokasi ad hoc dalam sistem untuk melacak jenis transaksi	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	tertentu yang menarik bagi organisasi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (a) (b) (c)	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1. Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2. Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c. Menyebarkan perangkat pemantauan: i. secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan (ii) di lokasi ad hoc dalam sistem untuk melacak jenis transaksi	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	tertentu yang menarik bagi organisasi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (a) (b) (c)	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1. Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2. Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c. Menyebarkan perangkat pemantauan: i. secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan (ii) di lokasi ad hoc dalam sistem untuk melacak jenis transaksi	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan rincian aktivitas panggilan API dalam AWS akun Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	tertentu yang menarik bagi organisasi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (a) (b) (c)	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1. Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2. Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c. Menyebarkan perangkat pemantauan: i. secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan (ii) di lokasi ad hoc dalam sistem untuk melacak jenis transaksi	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	tertentu yang menarik bagi organisasi.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (a) (b) (c)	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1. Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2. Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c. Menyebarkan perangkat pemantauan: i. secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan (ii) di lokasi ad hoc dalam sistem untuk melacak jenis transaksi	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindungnya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	tertentu yang menarik bagi organisasi.		
SI-7	Organisasi menggunakan alat verifikasi integritas untuk mendeteksi perubahan yang tidak sah pada [Penugasan: perangkat lunak, firmware, dan informasi yang ditentukan organisasi].	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (1)	Sistem informasi melakukan pemeriksaan integritas keamanan peristiwa yang relevan setidaknya setiap bulan.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (1)	Sistem informasi melakukan pemeriksaan integritas keamanan peristiwa yang relevan setidaknya setiap bulan.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (1)	Sistem informasi melakukan pemeriksaan integritas keamanan peristiwa yang relevan setidaknya setiap bulan.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RA-5 (1)	Organisasi ini menggunakan alat pemindaian kerentana n yang mencakup kemampuan untuk dengan mudah memperbarui kerentanan sistem informasi yang akan dipindai. Panduan Tambahan: Kerentanan yang akan dipindai perlu segera diperbaru i saat kerentana n baru ditemukan , diumumkan, dan metode pemindaia n dikembangkan. Proses pembaruan ini membantu memastika n bahwa potensi kerentanan dalam sistem informasi diidentifikasi dan ditangani secepat mungkin. Kontrol terkait: SI-3, SI-7.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RA-5 (1)	Organisasi ini menggunakan alat pemindaian kerentanan yang mencakup kemampuan untuk dengan mudah memperbarui kerentanan sistem informasi yang akan dipindai. Panduan Tambahan: Kerentanan yang akan dipindai perlu segera diperbarui saat kerentanan baru ditemukan, diumumkan, dan metode pemindaian dikembangkan. Proses pembaruan ini membantu memastikan bahwa potensi kerentanan dalam sistem informasi diidentifikasi dan ditangani secepat mungkin. Kontrol terkait: SI-3, SI-7.	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan: rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RA-5 (1)	Organisasi ini menggunakan alat pemindaian kerentana n yang mencakup kemampuan untuk dengan mudah memperbarui kerentanan sistem informasi yang akan dipindai. Panduan Tambahan: Kerentanan yang akan dipindai perlu segera diperbaru i saat kerentana n baru ditemukan , diumumkan, dan metode pemindaia n dikembangkan. Proses pembaruan ini membantu memastika n bahwa potensi kerentanan dalam sistem informasi diidentifikasi dan ditangani secepat mungkin. Kontrol terkait: SI-3, SI-7.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Organisasi: (a) Menerapkan antarmuka terkelola untuk setiap layanan telekomunikasi eksternal; (b) Menetapkan kebijakan arus lalu lintas untuk setiap antarmuka yang dikelola; (c) Melindungi kerahasiaan dan integritas informasi yang dikirimkan di setiap antarmuka; (d) Mendokumentasikan setiap pengecualian ke kebijakan arus lalu lintas dengan kebutuhan pendukung. mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business Panduan	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Tambahan: Kontrol terkait: SC-8.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Organisasi: (a) Menerapkan antarmuka terkelola untuk setiap layanan telekomunikasi eksternal; (b) Menetapkan kebijakan arus lalu lintas untuk setiap antarmuka yang dikelola; (c) Melindungi kerahasiaan dan integritas informasi yang dikirimkan di setiap antarmuka; (d) Mendokumentasikan setiap pengecualian ke kebijakan arus lalu lintas dengan kebutuhan pendukung. mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business Panduan	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Tambahan: Kontrol terkait: SC-8.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Organisasi: (a) Menerapkan antarmuka terkelola untuk setiap layanan telekomunikasi eksternal; (b) Menetapkan kebijakan arus lalu lintas untuk setiap antarmuka yang dikelola; (c) Melindungi kerahasiaan dan integritas informasi yang dikirimkan di setiap antarmuka; (d) Mendokumentasikan setiap pengecualian ke kebijakan arus lalu lintas dengan kebutuhan pendukung. mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business Panduan	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Tambahan: Kontrol terkait: SC-8.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Organisasi: (a) Menerapkan antarmuka terkelola untuk setiap layanan telekomunikasi eksternal; (b) Menetapkan kebijakan arus lalu lintas untuk setiap antarmuka yang dikelola; (c) Melindungi kerahasiaan dan integritas informasi yang dikirimkan di setiap antarmuka; (d) Mendokumentasikan setiap pengecualian ke kebijakan arus lalu lintas dengan kebutuhan pendukung. mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business Panduan	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Tambahan: Kontrol terkait: SC-8.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Organisasi: (a) Menerapkan antarmuka terkelola untuk setiap layanan telekomun ikasi eksternal ; (b) Menetapka n kebijakan arus lalu lintas untuk setiap antarmuka yang dikelola; (c) Melindungi kerahasia an dan integrita s informasi yang dikirimkan di setiap antarmuka; (d) Mendokumentasikan setiap pengecualian ke kebijakan arus lalu lintas dengan kebutuhan pendukung . mission/business need and duration of that need; and (e) Reviews exception s to the traffic flow policy [Assignment: organization-defin ed frequency] and removes exception s that are no longer supported by an explicit mission/b usiness Panduan	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Tambahan: Kontrol terkait: SC-8.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Organisasi: (a) Menerapkan antarmuka terkelola untuk setiap layanan telekomun ikasi eksternal ; (b) Menetapka n kebijakan arus lalu lintas untuk setiap antarmuka yang dikelola; (c) Melindungi kerahasia an dan integrita s informasi yang dikirimkan di setiap antarmuka; (d) Mendokumentasikan setiap pengecualian ke kebijakan arus lalu lintas dengan kebutuhan pendukung . mission/business need and duration of that need; and (e) Reviews exception s to the traffic flow policy [Assignment: organization-defin ed frequency] and removes exception s that are no longer supported by an explicit mission/b usiness Panduan	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Tambahan: Kontrol terkait: SC-8.		
SC-7 (5)	Sistem informasi pada antarmuka terkelola menyangkal lalu lintas komunikasi jaringan secara default dan memungkinkan lalu lintas komunikas i jaringan dengan pengecualian (yaitu, menolak semua, izin dengan pengecual ian). Panduan Tambahan: Peningkat an kontrol ini berlaku untuk lalu lintas komunikasi jaringan masuk dan keluar. Kebijakan lalu lintas komunikasi permit-by -exception jaringan yang menyangkal semua memastika n bahwa hanya koneksi yang penting dan disetujui yang diizinkan.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/ 0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (7)	Organisasi: (a) Menetapkan dan mengelola akun pengguna istimewa sesuai dengan skema akses berbasis peran yang mengatur akses sistem informasi yang diizinkan dan hak istimewa ke dalam peran; (b) Memantau tugas peran istimewa; dan (c) Mengambil [Penugasan: tindakan yang ditentukan organisasi] ketika tugas peran istimewa tidak lagi sesuai. Panduan Tambahan: Peran istimewa adalah peran yang ditentukan organisas i yang diberikan kepada individu yang memungkin kan individu tersebut melakukan fungsi tertentu yang relevan dengan keamanan yang tidak diizinkan oleh pengguna biasa. Peran istimewa ini termasuk, misalnya, manajemen kunci,	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	manajemen akun, administrasi jaringan dan sistem, administrasi basis data, dan administrasi web.		harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (7)	Organisasi: (a) Menetapkan dan mengelola akun pengguna istimewa sesuai dengan skema akses berbasis peran yang mengatur akses sistem informasi yang diizinkan dan hak istimewa ke dalam peran; (b) Memantau tugas peran istimewa; dan (c) Mengambil [Penugasan: tindakan yang ditentukan organisasi] ketika tugas peran istimewa tidak lagi sesuai. Panduan Tambahan: Peran istimewa adalah peran yang ditentukan organisasi yang diberikan kepada individu yang memungkinkan individu tersebut melakukan fungsi tertentu yang relevan dengan keamanan yang tidak diizinkan oleh pengguna biasa. Peran istimewa ini termasuk, misalnya, manajemen kunci,	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	manajemen akun, administrasi jaringan dan sistem, administrasi basis data, dan administrasi web.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (7)	Organisasi: (a) Menetapkan dan mengelola akun pengguna istimewa sesuai dengan skema akses berbasis peran yang mengatur akses sistem informasi yang diizinkan dan hak istimewa ke dalam peran; (b) Memantau tugas peran istimewa; dan (c) Mengambil [Penugasan: tindakan yang ditentukan organisasi] ketika tugas peran istimewa tidak lagi sesuai. Panduan Tambahan: Peran istimewa adalah peran yang ditentukan organisasi yang diberikan kepada individu yang memungkinkan individu tersebut melakukan fungsi tertentu yang relevan dengan keamanan yang tidak diizinkan oleh pengguna biasa. Peran istimewa ini termasuk, misalnya, manajemen kunci,	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	manajemen akun, administrasi jaringan dan sistem, administrasi basis data, dan administrasi web.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (7)	Organisasi: (a) Menetapkan dan mengelola akun pengguna istimewa sesuai dengan skema akses berbasis peran yang mengatur akses sistem informasi yang diizinkan dan hak istimewa ke dalam peran; (b) Memantau tugas peran istimewa; dan (c) Mengambil [Penugasan: tindakan yang ditentukan organisasi] ketika tugas peran istimewa tidak lagi sesuai. Panduan Tambahan: Peran istimewa adalah peran yang ditentukan organisasi yang diberikan kepada individu yang memungkinkan individu tersebut melakukan fungsi tertentu yang relevan dengan keamanan yang tidak diizinkan oleh pengguna biasa. Peran istimewa ini termasuk, misalnya, manajemen kunci,	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna IAM. Menempatkan pengguna IAM dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	manajemen akun, administrasi jaringan dan sistem, administrasi basis data, dan administrasi web.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (7)	Organisasi: (a) Menetapkan dan mengelola akun pengguna istimewa sesuai dengan skema akses berbasis peran yang mengatur akses sistem informasi yang diizinkan dan hak istimewa ke dalam peran; (b) Memantau tugas peran istimewa; dan (c) Mengambil [Penugasan: tindakan yang ditentukan organisasi] ketika tugas peran istimewa tidak lagi sesuai. Panduan Tambahan: Peran istimewa adalah peran yang ditentukan organisasi yang diberikan kepada individu yang memungkinkan individu tersebut melakukan fungsi tertentu yang relevan dengan keamanan yang tidak diizinkan oleh pengguna biasa. Peran istimewa ini termasuk, misalnya, manajemen kunci,	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi, pengembalian, dan pendelegasian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	manajemen akun, administrasi jaringan dan sistem, administrasi basis data, dan administrasi web.		harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (7)	Organisasi: (a) Menetapkan dan mengelola akun pengguna istimewa sesuai dengan skema akses berbasis peran yang mengatur akses sistem informasi yang diizinkan dan hak istimewa ke dalam peran; (b) Memantau tugas peran istimewa; dan (c) Mengambil [Penugasan: tindakan yang ditentukan organisasi] ketika tugas peran istimewa tidak lagi sesuai. Panduan Tambahan: Peran istimewa adalah peran yang ditentukan organisasi yang diberikan kepada individu yang memungkinkan individu tersebut melakukan fungsi tertentu yang relevan dengan keamanan yang tidak diizinkan oleh pengguna biasa. Peran istimewa ini termasuk, misalnya, manajemen kunci,	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	manajemen akun, administrasi jaringan dan sistem, administrasi basis data, dan administrasi web.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-11	Sistem informasi: a. Menghasilkan pesan kesalahan yang memberikan informasi yang diperlukan untuk tindakan korektif tanpa mengungkapkan informasi yang dapat dieksploitasi oleh musuh; dan b. Mengungkapkan pesan kesalahan hanya ke [Penugasan: personel atau peran yang ditentukan organisasi]. Panduan Tambahan: Organizations dengan hati-hati mempertimbangkan structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	attempts with passwords entered by mistake as the username, mission/business informasi yang dapat diperoleh dari (jika tidak dinyatakan secara eksplisit oleh) informasi yang direkam, dan informasi pribadi seperti nomor rekening, nomor jaminan sosial, dan nomor kartu kredit. Selain itu, pesan kesalahan dapat menyediak an saluran rahasia untuk mengirimkan informasi. Kontrol terkait: AU-2, AU-3, SC-31. Peningkatan Kontrol: Tidak ada. Referensi: Tidak ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-11	Sistem informasi: a. Menghasilkan pesan kesalahan yang memberikan informasi yang diperlukan untuk tindakan korektif tanpa mengungkapkan informasi yang dapat dieksploitasi oleh musuh; dan b. Mengungkapkan pesan kesalahan hanya ke [Penugasan: personel atau peran yang ditentukan organisasi]. Panduan Tambahan: Organizations dengan hati-hati mempertimbangkan structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	attempts with passwords entered by mistake as the username, mission/business informasi yang dapat diperoleh dari (jika tidak dinyatakan secara eksplisit oleh) informasi yang direkam, dan informasi pribadi seperti nomor rekening, nomor jaminan sosial, dan nomor kartu kredit. Selain itu, pesan kesalahan dapat menyediak an saluran rahasia untuk mengirimkan informasi. Kontrol terkait: AU-2, AU-3, SC-31. Peningkatan Kontrol: Tidak ada. Referensi: Tidak ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-11	Sistem informasi: a. Menghasilkan pesan kesalahan yang memberikan informasi yang diperlukan untuk tindakan korektif tanpa mengungka pkan informasi yang dapat dieksploitasi oleh musuh; dan b. Mengungkapkan pesan kesalahan hanya ke [Penugasa n: personel atau peran yang ditentukan organisasi]. Panduan Tambahan: Organizat ions dengan hati-hati mempertimbangkan structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operation al requirements. Information that could be exploited by adversaries includes, for example, erroneous logon	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	attempts with passwords entered by mistake as the username, mission/business informasi yang dapat diperoleh dari (jika tidak dinyatakan secara eksplisit oleh) informasi yang direkam, dan informasi pribadi seperti nomor rekening, nomor jaminan sosial, dan nomor kartu kredit. Selain itu, pesan kesalahan dapat menyediak an saluran rahasia untuk mengirimkan informasi. Kontrol terkait: AU-2, AU-3, SC-31. Peningkatan Kontrol: Tidak ada. Referensi: Tidak ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-11	Sistem informasi: a. Menghasilkan pesan kesalahan yang memberikan informasi yang diperlukan untuk tindakan korektif tanpa mengungkapkan informasi yang dapat dieksploitasi oleh musuh; dan b. Mengungkapkan pesan kesalahan hanya ke [Penugasan: personel atau peran yang ditentukan organisasi]. Panduan Tambahan: Organizations dengan hati-hati mempertimbangkan structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	attempts with passwords entered by mistake as the username, mission/business informasi yang dapat diperoleh dari (jika tidak dinyatakan secara eksplisit oleh) informasi yang direkam, dan informasi pribadi seperti nomor rekening, nomor jaminan sosial, dan nomor kartu kredit. Selain itu, pesan kesalahan dapat menyediak an saluran rahasia untuk mengirimkan informasi. Kontrol terkait: AU-2, AU-3, SC-31. Peningkatan Kontrol: Tidak ada. Referensi: Tidak ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-11	Sistem informasi: a. Menghasilkan pesan kesalahan yang memberikan informasi yang diperlukan untuk tindakan korektif tanpa mengungka pkan informasi yang dapat dieksploitasi oleh musuh; dan b. Mengungkapkan pesan kesalahan hanya ke [Penugasa n: personel atau peran yang ditentukan organisasi]. Panduan Tambahan: Organizat ions dengan hati-hati mempertimbangkan structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operation al requirements. Information that could be exploited by adversaries includes, for example, erroneous logon	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan rincian aktivitas panggilan API dalam AWS akun Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	attempts with passwords entered by mistake as the username, mission/business informasi yang dapat diperoleh dari (jika tidak dinyatakan secara eksplisit oleh) informasi yang direkam, dan informasi pribadi seperti nomor rekening, nomor jaminan sosial, dan nomor kartu kredit. Selain itu, pesan kesalahan dapat menyediak an saluran rahasia untuk mengirimkan informasi. Kontrol terkait: AU-2, AU-3, SC-31. Peningkatan Kontrol: Tidak ada. Referensi: Tidak ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-11	Sistem informasi: a. Menghasilkan pesan kesalahan yang memberikan informasi yang diperlukan untuk tindakan korektif tanpa mengungka pkan informasi yang dapat dieksploitasi oleh musuh; dan b. Mengungkapkan pesan kesalahan hanya ke [Penugasa n: personel atau peran yang ditentukan organisasi]. Panduan Tambahan: Organizat ions dengan hati-hati mempertimbangkan structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operation al requirements. Information that could be exploited by adversaries includes, for example, erroneous logon	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	attempts with passwords entered by mistake as the username, mission/business informasi yang dapat diperoleh dari (jika tidak dinyatakan secara eksplisit oleh) informasi yang direkam, dan informasi pribadi seperti nomor rekening, nomor jaminan sosial, dan nomor kartu kredit. Selain itu, pesan kesalahan dapat menyediak an saluran rahasia untuk mengirimkan informasi. Kontrol terkait: AU-2, AU-3, SC-31. Peningkatan Kontrol: Tidak ada. Referensi: Tidak ada.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-3	Organisasi: a. Menggunakan mekanisme perlindungan kode berbahaya pada titik masuk dan keluar sistem informasi untuk mendeteksi dan memberantas kode berbahaya ; b. Memperbarui mekanisme perlindungan kode berbahaya setiap kali rilis baru tersedia sesuai dengan kebijakan dan prosedur manajemen konfigurasi organisasi; c. Mengkonfigurasi mekanisme perlindungan kode berbahaya ke: 1. Lakukan pemindaian berkala dari sistem informasi [Penugasan: frekuensi yang ditentukan organisasi] dan pemindaian file secara real-time dari sumber eksternal di [Seleksi (satu atau lebih); titik akhir; entry/exit points] as the files	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild . Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	are downloaded, opened, or executed in accordance with organizational security policy; and 2. [Selection(one or more): block malicious code; quarantine malicious code; send alert to administr ator; [Assignment: organization-defined action]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availabil ity of the information system. Supplemental Guidance: Informati on system entry and exit points include, for example, firewalls , electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers , and mobile devices.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats(e .g., UUENCODE, Unicode), contained within compresse d or hidden files, or hidden in files using steganogr aphy. Malicious code can be transport ed by different means including, for example, web accesses, electroni c mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitat ion of information system vulnerabi lities. Malicious code protection mechanisms include, for example, anti-viru s signature definitio ns and reputation-based technologies.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example,		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	secure coding practices, configura tion managemen t and control, trusted procureme nt processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted . For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or tindakan jaringan dalam menanggap i deteksi kejahatan ketika mencoba membuka atau mengeksekusi file. Kontrol terkait: CM-3, MP-2, SA-4, SA-8,		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7. Referensi : Publikasi Khusus NIST 800-83.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-3	Organisasi: a. Menggunakan mekanisme perlindungan kode berbahaya pada titik masuk dan keluar sistem informasi untuk mendeteksi dan memberantas kode berbahaya ; b. Memperbarui mekanisme perlindungan kode berbahaya setiap kali rilis baru tersedia sesuai dengan kebijakan dan prosedur manajemen konfigurasi organisasi; c. Mengkonfigurasi mekanisme perlindungan kode berbahaya ke: 1. Lakukan pemindaian berkala dari sistem informasi [Penugasan: frekuensi yang ditentukan organisasi] dan pemindaian file secara real-time dari sumber eksternal di [Seleksi (satu atau lebih); titik akhir; entry/exit points] as the files	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, nama pengguna, dan kata sandi dalam lingkungan proyek AWS Codebuild. Gunakan OAuth alih-alih token akses pribadi atau nama pengguna dan kata sandi untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	are downloaded, opened, or executed in accordance with organizational security policy; and 2. [Selection(one or more): block malicious code; quarantine malicious code; send alert to administr ator; [Assignment: organization-defined action]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availabil ity of the information system. Supplemental Guidance: Informati on system entry and exit points include, for example, firewalls , electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers , and mobile devices.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats(e .g., UUENCODE, Unicode), contained within compresse d or hidden files, or hidden in files using steganogr aphy. Malicious code can be transport ed by different means including, for example, web accesses, electroni c mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitat ion of information system vulnerabi lities. Malicious code protection mechanisms include, for example, anti-viru s signature definitio ns and reputation-based technologies.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example,		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or tindakan jaringan dalam menanggapi deteksi kejahatan ketika mencoba membuka atau mengeksekusi file. Kontrol terkait: CM-3, MP-2, SA-4, SA-8,		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7. Referensi : Publikasi Khusus NIST 800-83.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-5	Organisasi: a. Menerima peringatan, nasihat, dan arahan keamanan sistem informasi dari [Penugasan: organisasi eksternal yang ditentukan organisasi] secara berkelanjutan; b. Menghasilkan peringatan keamanan internal, nasihat, dan arahan yang dianggap perlu; c. Menyebarluaskan peringatan keamanan, nasihat, dan arahan ke: [Seleksi (satu atau lebih): [Penugasan: personel atau peran yang ditentukan organisasi]; [Penugasan: elemen yang ditentukan organisasi dalam organisasi]; [Penugasan: organisasi eksternal yang ditentukan organisasi]]; dan d. Menerapkan arahan keamanan sesuai dengan kerangka	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	waktu yang ditetapkan, atau memberi tahu organisasi penerbit tentang tingkat ketidakpatuhan. Panduan Tambahan: Tim Kesiapan Darurat Komputer Amerika Serikat (US-CERT) menghasilkan peringatan dan nasihat keamanan untuk menjaga kesadaran situasional di seluruh pemerintah federal. Arahan keamanan dikeluarkan oleh OMB atau organisasi lain yang ditunjuk dengan tanggung jawab dan wewenang untuk mengeluarkan arahan tersebut. Kepatuhan terhadap arahan keamanan sangat penting karena sifat kritis dari banyak arahan ini dan potensi efek samping langsung pada operasi dan aset organisasi, individu, organisasi lain, dan Bangsa		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	jika arahan tidak dilaksanakan pada waktu yang tepat. Organisasi eksternal termasuk, misalnya, mission/business partners, supply chain partners, external service providers, and other peer/supporting organisasi eksternal . Kontrol terkait: SI-2. Referensi: Publikasi Khusus NIST 800-40.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-5	Organisasi: a. Menerima peringatan, nasihat, dan arahan keamanan sistem informasi dari [Penugasan: organisasi eksternal yang ditentukan organisasi] secara berkelanjutan; b. Menghasilkan peringatan keamanan internal, nasihat, dan arahan yang dianggap perlu; c. Menyebarluaskan peringatan keamanan, nasihat, dan arahan ke: [Seleksi (satu atau lebih): [Penugasan: personel atau peran yang ditentukan organisasi]; [Penugasan: elemen yang ditentukan organisasi dalam organisasi]; [Penugasan: organisasi eksternal yang ditentukan organisasi]]; dan d. Menerapkan arahan keamanan sesuai dengan kerangka	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	waktu yang ditetapkan, atau memberi tahu organisasi penerbit tentang tingkat ketidakpatuhan. Panduan Tambahan: Tim Kesiapan Darurat Komputer Amerika Serikat (US-CERT) menghasilkan peringatan dan nasihat keamanan untuk menjaga kesadaran situasional di seluruh pemerintah federal. Arahan keamanan dikeluarkan oleh OMB atau organisasi lain yang ditunjuk dengan tanggung jawab dan wewenang untuk mengeluarkan arahan tersebut. Kepatuhan terhadap arahan keamanan sangat penting karena sifat kritis dari banyak arahan ini dan potensi efek samping langsung pada operasi dan aset organisasi, individu, organisasi lain, dan Bangsa		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	jika arahan tidak dilaksanakan pada waktu yang tepat. Organisasi eksternal termasuk, misalnya, mission/business partners, supply chain partners, external service providers, and other peer/supporting organisasi eksternal . Kontrol terkait: SI-2. Referensi: Publikasi Khusus NIST 800-40.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-5	Organisasi: a. Menerima peringata n, nasihat, dan arahan keamanan sistem informasi dari [Penugasan: organisasi eksternal yang ditentukan organisasi] secara berkelanjutan; b. Menghasilkan peringatan keamanan internal, nasihat, dan arahan yang dianggap perlu; c. Menyebarluaskan peringatan keamanan, nasihat, dan arahan ke: [Seleksi (satu atau lebih): [Penugasan: personel atau peran yang ditentukan organisas i]; [Penugasa n: elemen yang ditentukan organisas i dalam organisas i]; [Penugasan: organisasi eksternal yang ditentukan organisasi]]; dan d. Menerapkan arahan keamanan sesuai dengan kerangka	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	waktu yang ditetapkan, atau memberi tahu organisasi penerbit tentang tingkat ketidakpatuhan. Panduan Tambahan: Tim Kesiapan Darurat Komputer Amerika Serikat (US-CERT) menghasilkan peringatan dan nasihat keamanan untuk menjaga kesadaran situasional di seluruh pemerintah federal. Arahan keamanan dikeluarkan oleh OMB atau organisasi lain yang ditunjuk dengan tanggung jawab dan wewenang untuk mengeluarkan arahan tersebut. Kepatuhan terhadap arahan keamanan sangat penting karena sifat kritis dari banyak arahan ini dan potensi efek samping langsung pada operasi dan aset organisasi, individu, organisasi lain, dan Bangsa		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	jika arahan tidak dilaksanakan pada waktu yang tepat. Organisasi eksternal termasuk, misalnya, mission/business partners, supply chain partners, external service providers, and other peer/supporting organisasi eksternal . Kontrol terkait: SI-2. Referensi: Publikasi Khusus NIST 800-40.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-5	Organisasi: a. Menerima peringatan, nasihat, dan arahan keamanan sistem informasi dari [Penugasan: organisasi eksternal yang ditentukan organisasi] secara berkelanjutan; b. Menghasilkan peringatan keamanan internal, nasihat, dan arahan yang dianggap perlu; c. Menyebarluaskan peringatan keamanan, nasihat, dan arahan ke: [Seleksi (satu atau lebih): [Penugasan: personel atau peran yang ditentukan organisasi]; [Penugasan: elemen yang ditentukan organisasi dalam organisasi]; [Penugasan: organisasi eksternal yang ditentukan organisasi]]; dan d. Menerapkan arahan keamanan sesuai dengan kerangka	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan: rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	waktu yang ditetapkan, atau memberi tahu organisasi penerbit tentang tingkat ketidakpatuhan. Panduan Tambahan: Tim Kesiapan Darurat Komputer Amerika Serikat (US-CERT) menghasilkan peringatan dan nasihat keamanan untuk menjaga kesadaran situasional di seluruh pemerintah federal. Arahan keamanan dikeluarkan oleh OMB atau organisasi lain yang ditunjuk dengan tanggung jawab dan wewenang untuk mengeluarkan arahan tersebut. Kepatuhan terhadap arahan keamanan sangat penting karena sifat kritis dari banyak arahan ini dan potensi efek samping langsung pada operasi dan aset organisasi, individu, organisasi lain, dan Bangsa		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	jika arahan tidak dilaksanakan pada waktu yang tepat. Organisasi eksternal termasuk, misalnya, mission/business partners, supply chain partners, external service providers, and other peer/supporting organisasi eksternal . Kontrol terkait: SI-2. Referensi: Publikasi Khusus NIST 800-40.		
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikasi, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisasi].	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di semua sistem informasi dan komponen jaringan di mana kemampuan audit disebarkan/tersedia c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa berikut: Kejadian login akun yang berhasil dan tidak berhasil, peristiwa manajemen akun, akses objek, perubahan kebijakan, fungsi hak istimewa, pelacakan proses, dan peristiwa sistem. Untuk aplikasi Web: semua aktivitas administrator, pemeriksaan otentikasi, pemeriksaan otorisasi, penghapusan data, akses data, perubahan data, dan perubahan izin. d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [subset yang ditentukan organisasi dari peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a untuk diaudit terus	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	menerus untuk setiap peristiwa yang diidentifikasi].		
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	codebuild-project-logging-enabled	Pastikan pencatata n AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatc h atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk FedRAMP (Bagian Tinggi 1).

Praktik Terbaik Operasional untuk FedRAMP (Bagian Tinggi 2)

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara Federal Risk and Authorization Management Program (FedRAMP) dan aturan Config terkelola. AWS Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau beberapa kontrol FedRAMP. Kontrol FedRAMP dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-02 (11)	Sistem informasi memberlakukan keadaan yang ditentukan organisasi dan/atau kondisi penggunaan untuk akun sistem yang ditentukan organisasi.	guardduty-enabled-centralized	Gunakan Amazon GuardDuty untuk memantau penggunaan kredenal jangka pendek yang terkait dengan peran instans IAM. Amazon GuardDuty dapat memeriksa eksfiltrasi kredensi di Profil Instans IAM menggunakan cek. UnauthorizedAccess
AC-02 (12) (a)	Organisasi: a. Memantau akun sistem informasi untuk [Penugasan: penggunaan atipikal yang ditentukan organisasi].	cloudtrail-security-trail-enabled	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan AWS akun yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
AC-06 (03)	Organisasi mengotorisasi akses jaringan ke personel yang ditugaskan hanya ketika diperlukan untuk menyelesaikan tugas untuk akses untuk rencana keamanan.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-06 (03)	Organisasi mengotorisasi akses jaringan ke [Penugasan: perintah istimewa yang ditentukan organisasi] hanya untuk [Penugasan: kebutuhan operasional menarik yang ditentukan organisasi] dan mendokumentasikan alasan untuk akses tersebut dalam rencana keamanan untuk sistem.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-06 (03)	Organisasi mengotorisasi akses jaringan ke [Penugasan: perintah istimewa yang ditentukan organisasi] hanya untuk [Penugasan: kebutuhan operasional menarik yang ditentukan organisasi] dan mendokumentasikan alasan untuk akses tersebut dalam rencana keamanan untuk sistem.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
AC-06 (03)	Organisasi mengotorisasi akses jaringan ke [Penugasan: perintah istimewa yang ditentukan organisasi] hanya untuk [Penugasan: kebutuhan operasional menarik yang ditentukan organisasi] dan mendokumentasikan alasan untuk akses tersebut dalam rencana keamanan untuk sistem.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-06 (03)	Organisasi mengotorisasi akses jaringan ke [Penugasan: perintah istimewa yang ditentukan organisasi] hanya untuk [Penugasan: kebutuhan operasional menarik yang ditentukan organisasi] dan mendokumentasikan alasan untuk akses tersebut dalam rencana keamanan untuk sistem.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-06 (03)	Organisasi mengotorisasi akses jaringan ke [Penugasan: perintah istimewa yang ditentukan organisasi] hanya untuk [Penugasan: kebutuhan operasional menarik yang ditentukan organisasi] dan mendokumentasikan alasan untuk akses tersebut dalam rencana keamanan untuk sistem.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-06 (03)	Organisasi mengotorisasi akses jaringan ke [Penugasan: perintah istimewa yang ditentukan organisasi] hanya untuk [Penugasan: kebutuhan operasional menarik yang ditentukan organisasi] dan mendokumentasikan alasan untuk akses tersebut dalam rencana keamanan untuk sistem.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
AC-06 (03)	Organisasi mengotorisasi akses jaringan ke [Penugasan: perintah istimewa yang ditentukan organisasi] hanya untuk [Penugasan: kebutuhan operasional menarik yang ditentukan organisasi] dan mendokumentasikan alasan untuk akses tersebut dalam rencana keamanan untuk sistem.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-06 (03)	Organisasi mengotorisasi akses jaringan ke [Penugasan: perintah istimewa yang ditentukan organisasi] hanya untuk [Penugasan: kebutuhan operasional menarik yang ditentukan organisasi] dan mendokumentasikan alasan untuk akses tersebut dalam rencana keamanan untuk sistem.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
AC-06 (03)	Organisasi mengotorisasi akses jaringan ke [Penugasan: perintah istimewa yang ditentukan organisasi] hanya untuk [Penugasan: kebutuhan operasional menarik yang ditentukan organisasi] dan mendokumentasikan alasan untuk akses tersebut dalam rencana keamanan untuk sistem.	eks-endpoint-no-public-akses	Kelola akses Anda ke klaster Amazon Elastic Kubernetes Service (Amazon EKS) dengan memastikan bahwa endpoint server Kubernetes API tidak dapat diakses publik. Dengan membatasi akses publik ke endpoint server API Kubernetes, Anda dapat mengurangi risiko akses tidak sah ke kluster EKS Anda dan sumber dayanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-05 (02)	Sistem informasi memberikan peringatan kepada personel kunci dalam waktu yang ditentukan ketika volume penyimpanan log audit yang dialokasikan mencapai persentase yang ditetapkan dari kapasitas penyimpanan log audit maksimum repositori.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-06 (04)	Tinjauan, Analisis, dan Pelaporan Catatan Audit | Tinjauan dan Analisis Pusat	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-06 (04)	Tinjauan, Analisis, dan Pelaporan Catatan Audit | Tinjauan dan Analisis Pusat	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-06 (04)	Tinjauan, Analisis, dan Pelaporan Catatan Audit | Tinjauan dan Analisis Pusat	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatata n AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
AU-06 (04)	Tinjauan, Analisis, dan Pelaporan Catatan Audit | Tinjauan dan Analisis Pusat	api-gw-execution-l ogging-diaktifkan	Pencatatan API Gateway menampilk an tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-06 (04)	Tinjauan, Analisis, dan Pelaporan Catatan Audit | Tinjauan dan Analisis Pusat	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan rincian aktivitas panggilan API dalam AWS akun Anda.
AU-06 (04)	Tinjauan, Analisis, dan Pelaporan Catatan Audit | Tinjauan dan Analisis Pusat	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan AWS akun yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-06 (04)	Tinjauan, Analisis, dan Pelaporan Catatan Audit | Tinjauan dan Analisis Pusat	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
AU-06 (04)	Tinjauan, Analisis, dan Pelaporan Catatan Audit | Tinjauan dan Analisis Pusat	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-06 (04)	Tinjauan, Analisis, dan Pelaporan Catatan Audit | Tinjauan dan Analisis Pusat	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-06 (04)	Tinjauan, Analisis, dan Pelaporan Catatan Audit | Tinjauan dan Analisis Pusat	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-06 (04)	Tinjauan, Analisis, dan Pelaporan Catatan Audit | Tinjauan dan Analisis Pusat	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-06 (04)	Tinjauan, Analisis, dan Pelaporan Catatan Audit | Tinjauan dan Analisis Pusat	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-06 (05)	Organisasi menginteg rasikan analisis catatan audit dengan analisis informasi pemindaian kerentana n, data kinerja, dan informasi pemantaua n sistem untuk lebih meningkat kan kemampuan mengidentifikasi aktivitas yang tidak pantas atau tidak biasa.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-06 (05)	Organisasi menginteg rasikan analisis catatan audit dengan analisis [Seleksi (satu atau lebih): informasi pemindaian kerentana n; data kinerja; informasi pemantaua n sistem; [Penugasa n: data/informasi yang ditentukan organisas i yang dikumpulkan dari sumber lain]] untuk lebih meningkat kan kemampuan mengidentifikasi aktivitas yang tidak pantas atau tidak biasa.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-06 (07)	Organisasi menentukan tindakan yang diizinkan untuk setiap proses sistem, peran, dan pengguna yang terkait dengan peninjauan, analisis, dan pelaporan informasi catatan audit.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-06 (07)	Organisasi menentukan tindakan yang diizinkan untuk setiap [Seleksi (satu atau lebih): proses sistem; peran; pengguna] yang terkait dengan tinjauan, analisis, dan pelaporan informasi catatan audit.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-09 (02)	Sistem informasi menerapkan mekanisme kriptografi untuk melindungi integritas informasi audit dan alat audit.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-09 (02)	Sistem informasi menerapkan mekanisme kriptografi untuk melindungi integritas informasi audit dan alat audit.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
AU-09 (02)	Sistem informasi menerapkan mekanisme kriptografi untuk melindungi integritas informasi audit dan alat audit.	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
AU-09 (02)	Sistem informasi menerapkan mekanisme kriptografi untuk melindungi integritas informasi audit dan alat audit.	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-09 (03)	Sistem informasi memberikan bukti tak terbantahkan yang telah dilakukan seseorang.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.
AU-09 (03)	Sistem informasi membatasi akses jaringan ke data log audit.	cloudtrail-s3- bucket-public-access-prohib ited	Memastikan bahwa bucket S3 yang digunakan untuk menyimpan CloudTrai l log tidak dapat diakses publik.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-10	Sistem informasi memberikan bukti yang tak terbantah kan bahwa seorang individu (atau proses yang bertindak atas nama individu) telah melakukan [Penugasa n: tindakan yang ditentukan organisas i yang akan dicakup oleh non-penolakan].	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan AWS akun yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
AU-10	Sistem informasi memberikan bukti yang tak terbantah kan bahwa seorang individu (atau proses yang bertindak atas nama individu) telah melakukan [Penugasa n: tindakan yang ditentukan organisas i yang akan dicakup oleh non-penolakan].	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrai l jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-10	Sistem informasi memberikan bukti yang tak terbantah kan bahwa seorang individu (atau proses yang bertindak atas nama individu) telah melakukan [Penugasa n: tindakan yang ditentukan organisas i yang akan dicakup oleh non-penolakan].	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Organisasi mengkompilasi catatan audit dari [Penugasan: komponen sistem yang ditentukan organisasi] ke dalam jejak audit seluruh sistem (logis atau fisik) yang berkorelasi waktu dengan dalam [Penugasan: tingkat toleransi yang ditentukan organisasi untuk hubungan antara stempel waktu catatan individu dalam jejak audit].	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Organisasi mengkompilasi catatan audit dari [Penugasan: komponen sistem yang ditentukan organisasi] ke dalam jejak audit seluruh sistem (logis atau fisik) yang berkorelasi waktu dengan dalam [Penugasan: tingkat toleransi yang ditentukan organisasi untuk hubungan antara stempel waktu catatan individu dalam jejak audit].	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Organisasi mengkompilasi catatan audit dari [Penugasan: komponen sistem yang ditentukan organisasi] ke dalam jejak audit seluruh sistem (logis atau fisik) yang berkorela si waktu dengan dalam [Penugasan: tingkat toleransi yang ditentukan organisas i untuk hubungan antara stempel waktu catatan individu dalam jejak audit].	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan rincian aktivitas panggilan API dalam AWS akun Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Organisasi mengkompilasi catatan audit dari [Penugasan: komponen sistem yang ditentukan organisasi] ke dalam jejak audit seluruh sistem (logis atau fisik) yang berkorela si waktu dengan dalam [Penugasan: tingkat toleransi yang ditentukan organisas i untuk hubungan antara stempel waktu catatan individu dalam jejak audit].	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan AWS akun yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Organisasi mengkompilasi catatan audit dari [Penugasan: komponen sistem yang ditentukan organisasi] ke dalam jejak audit seluruh sistem (logis atau fisik) yang berkorelasi waktu dengan dalam [Penugasan: tingkat toleransi yang ditentukan organisasi untuk hubungan antara stempel waktu catatan individu dalam jejak audit].	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Organisasi mengkompilasi catatan audit dari [Penugasan: komponen sistem yang ditentukan organisasi] ke dalam jejak audit seluruh sistem (logis atau fisik) yang berkorelasi waktu dengan dalam [Penugasan: tingkat toleransi yang ditentukan organisasi untuk hubungan antara stempel waktu catatan individu dalam jejak audit].	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Organisasi mengkompilasi catatan audit dari [Penugasan: komponen sistem yang ditentukan organisasi] ke dalam jejak audit seluruh sistem (logis atau fisik) yang berkorela si waktu dengan dalam [Penugasan: tingkat toleransi yang ditentukan organisas i untuk hubungan antara stempel waktu catatan individu dalam jejak audit].	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Organisasi mengkompilasi catatan audit dari [Penugasan: komponen sistem yang ditentukan organisasi] ke dalam jejak audit seluruh sistem (logis atau fisik) yang berkorela si waktu dengan dalam [Penugasan: tingkat toleransi yang ditentukan organisas i untuk hubungan antara stempel waktu catatan individu dalam jejak audit].	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Organisasi mengkompilasi catatan audit dari [Penugasan: komponen sistem yang ditentukan organisasi] ke dalam jejak audit seluruh sistem (logis atau fisik) yang berkorelasi waktu dengan dalam [Penugasan: tingkat toleransi yang ditentukan organisasi untuk hubungan antara stempel waktu catatan individu dalam jejak audit].	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-03	Organisasi menentukan dan mendokumentasikan jenis perubahan pada sistem yang dikontrol konfigurasi.	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-08 (02)	Organisasi mempertahankan mata uang, kelengkapan, akurasi, dan ketersediaan inventaris komponen sistem menggunakan [Penugasan: mekanisme otomatis yang ditentukan organisasi].	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-08 (02)	Organisasi mempertahankan mata uang, kelengkapan, akurasi, dan ketersediaan inventaris komponen sistem menggunakan [Penugasan: mekanisme otomatis yang ditentukan organisasi].	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-08 (02)	Organisasi mempertahankan mata uang, kelengkapan, akurasi, dan ketersediaan inventaris komponen sistem menggunakan [Penugasan: mekanisme otomatis yang ditentukan organisasi].	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-02 (05)	Orgainisasi menyediakan rencana untuk kelanjutan misi dan fungsi bisnis dengan kerugian minimal atau tidak ada kesinambu ngan operasional dan mempertah ankan kontinuitas itu sampai restorasi sistem penuh di lokasi pemrosesan dan/atau penyimpanan primer.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersedi aan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplika si data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastru ktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutk an operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-06 (02)	Organisasi mengkonfigurasi situs penyimpanan alternatif untuk memfasilitasi operasi pemulihan sesuai dengan waktu pemulihan dan tujuan titik pemulihan.	backup-recovery-point-minimum-pemeriksaan retensi	Memeriksa apakah titik pemulihan berakhir tidak lebih awal dari setelah periode yang ditentukan. Organizations menetapkan waktu pemulihan dan tujuan titik pemulihan sebagai bagian dari perencanaan kontingensi. Konfigurasi situs penyimpanan alternatif mencakup fasilitas fisik dan sistem yang mendukung operasi pemulihan yang memastikan aksesibilitas dan eksekusi yang benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-06 (02)	Organisasi mengkonfigurasi situs penyimpanan alternatif untuk memfasilitasi operasi pemulihan sesuai dengan waktu pemulihan dan tujuan titik pemulihan.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-06 (02)	Organisasi mengkonfigurasi situs penyimpanan alternatif untuk memfasilitasi operasi pemulihan sesuai dengan waktu pemulihan dan tujuan titik pemulihan.	rds-in-backup-plan	Memeriksa apakah database Amazon Relational Database Service (Amazon RDS) ada dalam AWS paket Backup. Organizations menetapkan waktu pemulihan dan tujuan titik pemulihan sebagai bagian dari perencanaan kontingensi. Konfigurasi situs penyimpanan alternatif mencakup fasilitas fisik dan sistem yang mendukung operasi pemulihan yang memastikan aksesibilitas dan eksekusi yang benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-06 (02)	Organisasi mengkonfigurasi situs penyimpanan alternatif untuk memfasilitasi operasi pemulihan sesuai dengan waktu pemulihan dan tujuan titik pemulihan.	dynamodb-in-backup-plan	Memeriksa apakah tabel Amazon DynamoDB ada di AWS Paket Cadangan. Organizations menetapkan waktu pemulihan dan tujuan titik pemulihan sebagai bagian dari perencanaan kontingensi. Konfigurasi situs penyimpanan alternatif mencakup fasilitas fisik dan sistem yang mendukung operasi pemulihan yang memastikan aksesibilitas dan eksekusi yang benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-06 (02)	Organisasi mengkonfigurasi situs penyimpanan alternatif untuk memfasilitasi operasi pemulihan sesuai dengan waktu pemulihan dan tujuan titik pemulihan.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-06 (02)	Organisasi mengkonfigurasi situs penyimpanan alternatif untuk memfasilitasi operasi pemulihan sesuai dengan waktu pemulihan dan tujuan titik pemulihan.	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-06 (02)	Organisasi mengkonfigurasi situs penyimpanan alternatif untuk memfasilitasi operasi pemulihan sesuai dengan waktu pemulihan dan tujuan titik pemulihan.	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-06 (02)	Organisasi mengkonfigurasi situs penyimpanan alternatif untuk memfasilitasi operasi pemulihan sesuai dengan waktu pemulihan dan tujuan titik pemulihan.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-06 (02)	Organisasi mengkonfigurasi situs penyimpanan alternatif untuk memfasilitasi operasi pemulihan sesuai dengan waktu pemulihan dan tujuan titik pemulihan.	s3- version-lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihkan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).
CP-06 (02)	Organisasi mengkonfigurasi situs penyimpanan alternatif untuk memfasilitasi operasi pemulihan sesuai dengan waktu pemulihan dan tujuan titik pemulihan.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-06 (02)	Organisasi mengkonfigurasi situs penyimpanan alternatif untuk memfasilitasi operasi pemulihan sesuai dengan waktu pemulihan dan tujuan titik pemulihan.	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-06 (02)	Organisasi mengkonfigurasi situs penyimpanan alternatif untuk memfasilitasi operasi pemulihan sesuai dengan waktu pemulihan dan tujuan titik pemulihan.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-06 (02)	Organisasi mengkonfigurasi situs penyimpanan alternatif untuk memfasilitasi operasi pemulihan sesuai dengan waktu pemulihan dan tujuan titik pemulihan.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-06 (02)	Organisasi mengkonfigurasi situs penyimpanan alternatif untuk memfasilitasi operasi pemulihan sesuai dengan waktu pemulihan dan tujuan titik pemulihan.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-06 (02)	Organisasi mengkonfigurasi situs penyimpanan alternatif untuk memfasilitasi operasi pemulihan sesuai dengan waktu pemulihan dan tujuan titik pemulihan.	s3- bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-06 (02)	Organisasi mengkonfigurasi situs penyimpanan alternatif untuk memfasilitasi operasi pemulihan sesuai dengan waktu pemulihan dan tujuan titik pemulihan.	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-07 (01)	Orgainisasi mengidentifikasi situs pemrosesan alternatif yang cukup terpisah dari situs pemrosesan utama untuk mengurangi kerentanan terhadap ancaman yang sama.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-07 (04)	Organisasi menyiapkan situs pemrosesan alternatif sehingga situs dapat berfungsi sebagai situs operasional yang mendukung misi penting dan fungsi bisnis.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-07 (04)	Organisasi menyiapkan situs pemrosesan alternatif sehingga situs dapat berfungsi sebagai situs operasional yang mendukung misi penting dan fungsi bisnis.	backup-recovery-point-encrypted	Memeriksa apakah titik pemulihan dienkripsi. Persiapan lokasi termasuk menetapkan pengaturan konfigurasi untuk sistem di lokasi pemrosesan alternatif yang konsisten dengan persyaratan untuk pengaturan tersebut di lokasi utama dan memastikan bahwa persediaan penting dan pertimbangan logistik ada.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-07 (04)	Organisasi menyiapkan situs pemrosesan alternatif sehingga situs dapat berfungsi sebagai situs operasional yang mendukung misi penting dan fungsi bisnis.	backup-recovery-point-manual-penghapusan-dinonaktifkan	Memeriksa apakah brankas cadangan memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Persiapan lokasi termasuk menetapkan pengaturan konfigurasi untuk sistem di lokasi pemrosesan alternatif yang konsisten dengan persyaratan untuk pengaturan tersebut di lokasi utama dan memastikan bahwa persediaan penting dan pertimbangan logistik ada.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-07 (04)	Organisasi menyiapkan situs pemrosesan alternatif sehingga situs dapat berfungsi sebagai situs operasional yang mendukung misi penting dan fungsi bisnis.	s3- -diaktifkan bucket-cross-region-replication	Memeriksa apakah Anda telah mengaktifkan Replikasi Lintas Wilayah S3 untuk bucket Amazon S3 Anda. Persiapan lokasi termasuk menetapkan pengaturan konfigurasi untuk sistem di lokasi pemrosesan alternatif yang konsisten dengan persyaratan untuk pengaturan tersebut di lokasi utama dan memastikan bahwa persediaan penting dan pertimbangan logistik ada.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-09 (03)	Organisasi menyimpan salinan cadangan [Penugasan: perangkat lunak sistem kritis yang ditentukan organisasi dan informasi terkait keamanan lainnya] di fasilitas terpisah atau dalam wadah pengenal api yang tidak ditempatkan dengan sistem operasional.	backup-recovery-point-minimum-pemeriksaan retensi	Memeriksa apakah titik pemulihan berakhir tidak lebih awal dari setelah periode yang ditentukan. Penyimpanan terpisah untuk informasi penting berlaku untuk semua informasi penting terlepas dari jenis media penyimpanan cadangan. Perangkat lunak sistem kritis meliputi sistem operasi, middleware, sistem manajemen kunci kriptografi, dan sistem deteksi intrusi. Informasi terkait keamanan mencakup inventaris perangkat keras sistem, perangkat lunak, dan komponen firmware. Situs penyimpanan alternatif, termasuk arsitektur yang didistribusikan secara geografis, berfungsi sebagai fasilitas penyimpanan terpisah untuk

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			organisasi. Organizations dapat menyediakan penyimpanan terpisah dengan menerapkan proses pencadangan otomatis di situs penyimpanan alternatif (misalnya, pusat data). Administrasi Layanan Umum (GSA) menetapkan standar dan spesifikasi untuk keamanan dan kontainer dengan nilai kebakaran.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-09 (03)	Organisasi menyimpan salinan cadangan [Penugasan: perangkat lunak sistem kritis yang ditentukan organisasi dan informasi terkait keamanan lainnya] di fasilitas terpisah atau dalam wadah pengenal api yang tidak ditempatkan dengan sistem operasional.	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-09 (03)	Organisasi menyimpan salinan cadangan [Penugasan: perangkat lunak sistem kritis yang ditentukan organisasi dan informasi terkait keamanan lainnya] di fasilitas terpisah atau dalam wadah pengenal api yang tidak ditempatkan dengan sistem operasional.	ebs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-09 (03)	Organisasi menyimpan salinan cadangan [Penugasan: perangkat lunak sistem kritis yang ditentukan organisasi dan informasi terkait keamanan lainnya] di fasilitas terpisah atau dalam wadah pengenal api yang tidak ditempatkan dengan sistem operasional.	efs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-09 (03)	Organisasi menyimpan salinan cadangan [Penugasan: perangkat lunak sistem kritis yang ditentukan organisasi dan informasi terkait keamanan lainnya] di fasilitas terpisah atau dalam wadah pengenal api yang tidak ditempatkan dengan sistem operasional.	rds-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Relational Database Service (Amazon RDS) Anda merupakan AWS bagian dari paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-09 (03)	Organisasi menyimpan salinan cadangan [Penugasan: perangkat lunak sistem kritis yang ditentukan organisasi dan informasi terkait keamanan lainnya] di fasilitas terpisah atau dalam wadah pengenal api yang tidak ditempatkan dengan sistem operasional.	s3- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-09 (03)	Organisasi menyimpan salinan cadangan [Penugasan: perangkat lunak sistem kritis yang ditentukan organisasi dan informasi terkait keamanan lainnya] di fasilitas terpisah atau dalam wadah pengenal api yang tidak ditempatkan dengan sistem operasional.	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-09 (03)	Organisasi menyimpan salinan cadangan [Penugasan: perangkat lunak sistem kritis yang ditentukan organisasi dan informasi terkait keamanan lainnya] di fasilitas terpisah atau dalam wadah pengenal api yang tidak ditempatkan dengan sistem operasional.	dynamodb-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-09 (03)	Organisasi menyimpan salinan cadangan [Penugasan: perangkat lunak sistem kritis yang ditentukan organisasi dan informasi terkait keamanan lainnya] di fasilitas terpisah atau dalam wadah pengenal api yang tidak ditempatkan dengan sistem operasional.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-09 (03)	Organisasi menyimpan salinan cadangan [Penugasan: perangkat lunak sistem kritis yang ditentukan organisasi dan informasi terkait keamanan lainnya] di fasilitas terpisah atau dalam wadah pengenal api yang tidak ditempatkan dengan sistem operasional.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-09 (05)	Organisasi mentransfer informasi cadangan sistem ke situs penyimpanan alternatif [Penugasan: periode waktu yang ditentukan organisasi dan kecepatan transfer yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan].	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.
CP-09 (05)	Organisasi mentransfer informasi cadangan sistem ke situs penyimpanan alternatif [Penugasan: periode waktu yang ditentukan organisasi dan kecepatan transfer yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan].	backup-recovery-point-minimum-pemeriksaan retensi	Memeriksa apakah titik pemulihan berakhir tidak lebih awal dari setelah periode yang ditentukan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-09 (05)	Organisasi mentransfer informasi cadangan sistem ke situs penyimpanan alternatif [Penugasan: periode waktu yang ditentukan organisasi dan kecepatan transfer yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan].	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-09 (05)	Organisasi mentransfer informasi cadangan sistem ke situs penyimpanan alternatif [Penugasan: periode waktu yang ditentukan organisasi dan kecepatan transfer yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan].	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-09 (05)	Organisasi mentransfer informasi cadangan sistem ke situs penyimpanan alternatif [Penugasan: periode waktu yang ditentukan organisasi dan kecepatan transfer yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan].	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-09 (08)	Organisasi menggunakan mekanisme kriptografi untuk mencegah informasi cadangan pengungkapan yang tidak sah.	backup-recovery-point-encrypted	Pemilihan mekanisme kriptografi didasarkan pada kebutuhan untuk melindungi kerahasiaan dan integritas informasi cadangan. Kekuatan mekanisme yang dipilih sepadan dengan kategori keamanan atau klasifikasi informasi. Perlindungan kriptografi berlaku untuk informasi cadangan sistem dalam penyimpanan di lokasi primer dan alternatif. Organizations yang menerapkan mekanisme kriptografi untuk melindungi informasi pada saat istirahat juga mempertimbangkan solusi manajemen kunci kriptografi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10 (04)	Organisasi menyediakan kemampuan untuk memulihkan komponen sistem dalam [Penugasan: periode waktu pemulihan yang ditentukan organisasi] dari informasi yang dikontrol konfigurasi dan dilindungi integritas yang mewakili keadaan operasional yang diketahui untuk komponen.	backup-recovery-point-encrypted	Aktifkan aturan ini untuk memeriksa apakah titik pemulihan dienkripsi.
CP-10 (04)	Organisasi menyediakan kemampuan untuk memulihkan komponen sistem dalam [Penugasan: periode waktu pemulihan yang ditentukan organisasi] dari informasi yang dikontrol konfigurasi dan dilindungi integritas yang mewakili keadaan operasional yang diketahui untuk komponen.	backup-recovery-point-minimum-pemeriksaan retensi	Aktifkan aturan ini untuk memastikan bahwa jika titik pemulihan berakhir tidak lebih baik daripada setelah periode yang ditentukan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10 (04)	Organisasi menyediakan kemampuan untuk memulihkan komponen sistem dalam [Penugasan: periode waktu pemulihan yang ditentukan organisasi] dari informasi yang dikontrol konfigurasi dan dilindungi integritas yang mewakili keadaan operasional yang diketahui untuk komponen.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10 (04)	Organisasi menyediakan kemampuan untuk memulihkan komponen sistem dalam [Penugasan: periode waktu pemulihan yang ditentukan organisasi] dari informasi yang dikontrol konfigurasi dan dilindungi integritas yang mewakili keadaan operasional yang diketahui untuk komponen.	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10 (04)	Organisasi menyediakan kemampuan untuk memulihkan komponen sistem dalam [Penugasan: periode waktu pemulihan yang ditentukan organisasi] dari informasi yang dikontrol konfigurasi dan dilindungi integritas yang mewakili keadaan operasional yang diketahui untuk komponen.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-02 (02)	Menerapkan otentikasi multi-faktor untuk akses ke akun yang tidak memiliki hak istimewa.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-02 (02)	Menerapkan otentikasi multi-faktor untuk akses ke akun yang tidak memiliki hak istimewa.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-02 (06)	Sistem informasi Menerapkan otentikasi multi-faktor untuk [Seleksi (satu atau lebih): lokal; jaringan; jarak jauh] akses ke [Seleksi (satu atau lebih): akun istimewa; akun yang tidak memiliki hak istimewa] sedemikian rupa sehingga: (a) Salah satu faktor disediakan oleh perangkat yang terpisah dari sistem yang mendapatkan akses; dan (b) Perangkat memenuhi [Penugasan: kekuatan persyaratan mekanisme yang ditentukan organisasi].	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-02 (06)	Sistem informasi Menerapkan otentikasi multi-faktor untuk [Seleksi (satu atau lebih): lokal; jaringan; jarak jauh] akses ke [Seleksi (satu atau lebih): akun istimewa; akun yang tidak memiliki hak istimewa] sedemikian rupa sehingga: (a) Salah satu faktor disediakan oleh perangkat yang terpisah dari sistem yang mendapatkan akses; dan (b) Perangkat memenuhi [Penugasan: kekuatan persyaratan mekanisme yang ditentukan organisasi].	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-02 (08)	Sistem informasi mengimplementasikan mekanisme otentikasi tahan replay untuk akses ke [Seleksi (satu atau lebih): akun istimewa; akun yang tidak memiliki hak istimewa].	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-05 (08)	Sistem informasi mengimplementasikan [Penugasan: kontrol keamanan yang ditentukan organisasi] untuk mengelola risiko kompromi karena individu memiliki akun di beberapa sistem.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-05 (08)	Sistem informasi mengimplementasikan [Penugasan: kontrol keamanan yang ditentukan organisasi] untuk mengelola risiko kompromi karena individu memiliki akun di beberapa sistem.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna IAM. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna IAM.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-05 (08)	Sistem informasi mengimplementasikan [Penugasan: kontrol keamanan yang ditentukan organisasi] untuk mengelola risiko kompromi karena individu memiliki akun di beberapa sistem.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebagai gantinya, buat dan gunakan AWS akun berbasis peran untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-05 (08)	Sistem informasi mengimplementasikan [Penugasan: kontrol keamanan yang ditentukan organisasi] untuk mengelola risiko kompromi karena individu memiliki akun di beberapa sistem.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-05 (08)	Sistem informasi mengimplementasikan [Penugasan: kontrol keamanan yang ditentukan organisasi] untuk mengelola risiko kompromi karena individu memiliki akun di beberapa sistem.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-05 (08)	Sistem informasi mengimplementasikan [Penugasan: kontrol keamanan yang ditentukan organisasi] untuk mengelola risiko kompromi karena individu memiliki akun di beberapa sistem.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna IAM adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-04 (04)	Organisasi ini menggunakan mekanisme otomatis untuk mengkorel asikan informasi insiden dan respons insiden individu untuk mencapai perspekti f seluruh organisas i tentang kesadaran dan respons insiden.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-04 (04)	Organisasi ini menggunakan mekanisme otomatis untuk mengkorel asikan informasi insiden dan respons insiden individu untuk mencapai perspekti f seluruh organisas i tentang kesadaran dan respons insiden.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
IR-04 (04)	Organisasi ini menggunakan mekanisme otomatis untuk mengkorel asikan informasi insiden dan respons insiden individu untuk mencapai perspekti f seluruh organisas i tentang kesadaran dan respons insiden.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteks i aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-04 (04)	Organisasi ini menggunakan mekanisme otomatis untuk mengkorel asikan informasi insiden dan respons insiden individu untuk mencapai perspekti f seluruh organisas i tentang kesadaran dan respons insiden.	cloudwatch-alarm-a ction-check	Amazon CloudWatc h mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasark an pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActi onRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-04 (04)	Organisasi ini menggunakan mekanisme otomatis untuk mengkorel asikan informasi insiden dan respons insiden individu untuk mencapai perspekti f seluruh organisas i tentang kesadaran dan respons insiden.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan rincian aktivitas panggilan API dalam AWS akun Anda.
RA-05	Memantau dan memindai kerentana n aplikasi yang dihosting dan ketika kerentana n baru berpotensi mempengaruhi sistem diidentifikasi dan dilaporkan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RA-05	Tentukan luas dan kedalaman cakupan pemindaian kerentanan.	inspector-lambda-standard-scan-diaktifkan	Memeriksa apakah pemindaian standar Amazon Inspector V2 Lambda diaktifkan untuk lingkungan tunggal atau multi-akun Anda untuk mendeteksi potensi kerentanan perangkat lunak. Aturannya adalah NON_COMPLIANT jika pemindaian standar Lambda tidak diaktifkan.
RA-05	Tentukan luas dan kedalaman cakupan pemindaian kerentanan.	inspector-ec2-scan-enabled	Memeriksa apakah EC2 pemindaian Amazon Inspector V2 diaktifkan untuk lingkungan tunggal atau multi-akun Anda guna mendeteksi potensi kerentanan dan masalah jangkauan jaringan pada instans Anda. EC2 Aturannya adalah NON_COMPLIANT jika EC2 pemindaian tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RA-05	Tentukan luas dan kedalaman cakupan pemindaian kerentanan.	inspector-ecr-scan-enabled	Memeriksa apakah pemindaian Amazon Inspector V2 ECR diaktifkan untuk lingkungan tunggal atau multi-akun Anda untuk mendeteksi potensi kerentanan perangkat lunak dalam gambar kontainer Anda. Aturannya adalah NON_COMPLIANT jika pemindaian ECR tidak diaktifkan.
RA-05 (03)	Tentukan luas dan kedalaman cakupan pemindaian kerentanan.	inspector-lambda-standard-scan-diaktifkan	Memeriksa apakah pemindaian standar Amazon Inspector V2 Lambda diaktifkan untuk lingkungan tunggal atau multi-akun Anda untuk mendeteksi potensi kerentanan perangkat lunak. Aturannya adalah NON_COMPLIANT jika pemindaian standar Lambda tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RA-05 (03)	Tentukan luas dan kedalaman cakupan pemindaian kerentana n.	inspector-ec2-scan-enabled	Memeriksa apakah EC2 pemindaian Amazon Inspector V2 diaktifkan untuk lingkungan tunggal atau multi-akun Anda guna mendeteksi potensi kerentana n dan masalah jangkauan jaringan pada instans Anda. EC2 Aturannya adalah NON_COMPL IANT jika EC2 pemindaian tidak diaktifkan.
RA-05 (03)	Tentukan luas dan kedalaman cakupan pemindaian kerentana n.	inspector-ecr-scan-enabled	Memeriksa apakah pemindaian Amazon Inspector V2 ECR diaktifkan untuk lingkungan tunggal atau multi-akun Anda untuk mendeteksi potensi kerentana n perangkat lunak dalam gambar kontainer Anda. Aturannya adalah NON_COMPLIANT jika pemindaian ECR tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RA-05 (05)	Menerapkan otorisasi akses istimewa ke [Penugasan: komponen sistem yang ditentukan organisasi] untuk pemindaian organisasi. (Menentukan semua komponen yang mendukung otentikasi dan semua scan)	inspector-ec2-scan-enabled	Memeriksa apakah EC2 pemindaian Amazon Inspector V2 diaktifkan untuk lingkungan tunggal atau multi-akun Anda guna mendeteksi potensi kerentanan dan masalah jangkauan jaringan pada instans Anda. EC2 Aturannya adalah NON_COMPLIANT jika EC2 pemindaian tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-10	Orgainisasi mengharuskan pengembang sistem, komponen sistem, atau layanan sistem untuk: a. Melakukan manajemen konfigura si selama sistem, komponen, atau layanan [Seleksi (satu atau lebih): desain; pengemban gan; implementasi; operasi; pembuanga n]; b. Mendokume ntasikan, mengelola , dan mengontrol integritas perubahan pada [Penugasa n: item konfigura si yang ditentukan organisasi di bawah manajemen konfigura si]; c. Menerapkan hanya perubahan yang disetujui organisasi pada sistem, komponen, atau layanan; d. Mendokumentasikan perubahan yang disetujui pada sistem, komponen, atau layanan dan	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	potensi dampak keamanan dan privasi dari perubahan tersebut; dan e. Lacak kelemahan keamanan dan resolusi cacat dalam sistem, komponen, atau layanan dan laporkan temuan ke [Penugasan: personel yang ditentukan organisasi].		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-07 (12)	Orgainisasi mengimplementasikan [Penugasan: mekanisme perlindungan batas berbasis host yang ditentukan organisasi] di [Penugasan: komponen sistem yang ditentukan organisasi].	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-07 (20)	Menyediakan kemampuan untuk secara dinamis mengisolasi [Penugasan: komponen sistem yang ditentukan organisasi] dari komponen sistem lainnya.	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-07 (21)	Gunakan mekanisme perlindungan batas untuk mengisola si [Penugasan: komponen sistem yang ditentuka n organisasi] yang mendukung [Penugasan: misi yang ditentukan organisasi dan/atau fungsi bisnis].	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-07 (21)	Gunakan mekanisme perlindungan batas untuk mengisola si [Penugasan: komponen sistem yang ditentuka n organisasi] yang mendukung [Penugasan: misi yang ditentukan organisasi dan/atau fungsi bisnis].	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-12 (01)	Menetapkan dan mengelola kunci kriptografi ketika kriptografi digunakan dalam sistem sesuai dengan persyaratan manajemen kunci berikut: [Penugasan: persyaratan yang ditentukan organisasi untuk pembuatan kunci, distribusi, penyimpanan, akses, dan penghancuran].	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan AWS akun yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28 (01)	Orgainisasi mengimplementasikan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi informasi berikut yang tidak sah pada [Penugasan: komponen atau media sistem yang ditentukan organisasi]: [Penugasan: informasi yang ditentukan organisasi].	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
SC-28 (01)	Orgainisasi mengimplementasikan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi informasi berikut yang tidak sah pada [Penugasan: komponen atau media sistem yang ditentukan organisasi]: [Penugasan: informasi yang ditentukan organisasi].	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28 (01)	Orgainisasi mengimplementasikan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi informasi berikut yang tidak sah pada [Penugasan: komponen atau media sistem yang ditentukan organisasi]: [Penugasan: informasi yang ditentukan organisasi].	kinesis-stream-encrypted	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.
SC-28 (01)	Orgainisasi mengimplementasikan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi informasi berikut yang tidak sah pada [Penugasan: komponen atau media sistem yang ditentukan organisasi]: [Penugasan: informasi yang ditentukan organisasi].	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28 (01)	Orgainisasi mengimplementasikan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi informasi berikut yang tidak sah pada [Penugasan: komponen atau media sistem yang ditentukan organisasi]: [Penugasan: informasi yang ditentukan organisasi].	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-28 (01)	Orgainisasi mengimplementasikan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi informasi berikut yang tidak sah pada [Penugasan: komponen atau media sistem yang ditentukan organisasi]: [Penugasan: informasi yang ditentukan organisasi].	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28 (01)	Orgainisasi mengimplementasikan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi informasi berikut yang tidak sah pada [Penugasan: komponen atau media sistem yang ditentukan organisasi]: [Penugasan: informasi yang ditentukan organisasi].	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28 (01)	Orgainisasi mengimplementasikan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi informasi berikut yang tidak sah pada [Penugasan: komponen atau media sistem yang ditentukan organisasi]: [Penugasan: informasi yang ditentukan organisasi].	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-28 (01)	Orgainisasi mengimplementasikan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi informasi berikut yang tidak sah pada [Penugasan: komponen atau media sistem yang ditentukan organisasi]: [Penugasan: informasi yang ditentukan organisasi].	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28 (01)	Orgainisasi mengimplementasikan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi informasi berikut yang tidak sah pada [Penugasan: komponen atau media sistem yang ditentukan organisasi]: [Penugasan: informasi yang ditentukan organisasi].	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
SC-28 (01)	Orgainisasi mengimplementasikan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi informasi berikut yang tidak sah pada [Penugasan: komponen atau media sistem yang ditentukan organisasi]: [Penugasan: informasi yang ditentukan organisasi].	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28 (01)	Orgainisasi mengimplementasikan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi informasi berikut yang tidak sah pada [Penugasan: komponen atau media sistem yang ditentukan organisasi]: [Penugasan: informasi yang ditentukan organisasi].	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
SC-28 (01)	Orgainisasi mengimplementasikan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi informasi berikut yang tidak sah pada [Penugasan: komponen atau media sistem yang ditentukan organisasi]: [Penugasan: informasi yang ditentukan organisasi].	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28 (01)	Orgainisasi mengimplementasikan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi informasi berikut yang tidak sah pada [Penugasan: komponen atau media sistem yang ditentukan organisasi]: [Penugasan: informasi yang ditentukan organisasi].	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28 (01)	Orgainisasi mengimplementasikan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi informasi berikut yang tidak sah pada [Penugasan: komponen atau media sistem yang ditentukan organisasi]: [Penugasan: informasi yang ditentukan organisasi].	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-28 (01)	Orgainisasi mengimplementasikan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi informasi berikut yang tidak sah pada [Penugasan: komponen atau media sistem yang ditentukan organisasi]: [Penugasan: informasi yang ditentukan organisasi].	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28 (01)	Orgainisasi mengimplementasikan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi informasi berikut yang tidak sah pada [Penugasan: komponen atau media sistem yang ditentukan organisasi]: [Penugasan: informasi yang ditentukan organisasi].	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-28 (01)	Orgainisasi mengimplementasikan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi informasi berikut yang tidak sah pada [Penugasan: komponen atau media sistem yang ditentukan organisasi]: [Penugasan: informasi yang ditentukan organisasi].	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-04 (12)	Peringatan [Penugasan: personel atau peran yang ditentukan organisasi] menggunakan [Penugasan: mekanisme otomatis yang ditentukan organisasi] ketika indikasi aktivitas yang tidak pantas atau tidak biasa berikut dengan implikasi keamanan atau privasi terjadi: [Penugasan: aktivitas yang ditentukan organisasi yang memicu peringatan].	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-04 (20)	Terapkan pemantauan tambahan berikut dari pengguna istimewa: [Penugasan: pemantauan tambahan yang ditentukan organisasi].	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-04 (20)	Terapkan pemantauan tambahan berikut dari pengguna istimewa: [Penugasan: pemantauan tambahan yang ditentukan organisasi].	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-04 (20)	Terapkan pemantauan tambahan berikut dari pengguna istimewa: [Penugasan: pemantauan tambahan yang ditentukan organisasi].	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-04 (20)	Terapkan pemantauan tambahan berikut dari pengguna istimewa: [Penugasan: pemantauan tambahan yang ditentukan organisasi].	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan rincian aktivitas panggilan API dalam AWS akun Anda.
SI-04 (20)	Terapkan pemantauan tambahan berikut dari pengguna istimewa: [Penugasan: pemantauan tambahan yang ditentukan organisasi].	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan AWS akun yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-04 (20)	Terapkan pemantauan tambahan berikut dari pengguna istimewa: [Penugasan: pemantauan tambahan yang ditentukan organisasi].	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
SI-04 (20)	Terapkan pemantauan tambahan berikut dari pengguna istimewa: [Penugasan: pemantauan tambahan yang ditentukan organisasi].	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-04 (20)	Terapkan pemantauan tambahan berikut dari pengguna istimewa: [Penugasan: pemantauan tambahan yang ditentukan organisasi].	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-04 (20)	Terapkan pemantauan tambahan berikut dari pengguna istimewa: [Penugasan: pemantauan tambahan yang ditentukan organisasi].	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-04 (22)	(a) Mendeteksi layanan jaringan yang belum disahkan atau disetujui oleh [Penugasan: proses otorisasi atau persetujuan yang ditentukan organisasi]; dan (b) [Seleksi (satu atau lebih): Audit; Peringatan [Penugasan: personel atau peran yang ditentukan organisasi]] ketika terdeteksi.	Securityhub-enabled	(A) AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-04 (22)	(a) Mendeteksi layanan jaringan yang belum disahkan atau disetujui oleh [Penugasan: proses otorisasi atau persetujuan yang ditentukan organisasi]; dan (b) [Seleksi (satu atau lebih): Audit; Peringatan [Penugasan: personel atau peran yang ditentukan organisasi]] ketika terdeteksi.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-04 (22)	(a) Mendeteksi layanan jaringan yang belum disahkan atau disetujui oleh [Penugasan: proses otorisasi atau persetujuan yang ditentukan organisasi]; dan (b) [Seleksi (satu atau lebih): Audit; Peringatan [Penugasan: personel atau peran yang ditentukan organisasi]] ketika terdeteksi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-05 (01)	Siarkan peringata n keamanan dan informasi penasihat di seluruh organisas i menggunak an [Penugasan: mekanisme otomatis yang ditentukan organisasi].	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-05 (01)	Siarkan peringata n keamanan dan informasi penasihat di seluruh organisas i menggunak an [Penugasan: mekanisme otomatis yang ditentukan organisasi].	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-07 (02)	Gunakan alat otomatis yang memberikan pemberitahuan kepada [Penugasan: personel atau peran yang ditentukan organisasi] setelah menemukan perbedaan selama verifikasi integritas.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-07 (02)	Gunakan alat otomatis yang memberikan pemberitahuan kepada [Penugasan: personel atau peran yang ditentukan organisasi] setelah menemukan perbedaan selama verifikasi integritas.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-07 (05)	Secara otomatis [Seleksi (satu atau lebih): matikan sistem; restart sistem; menerapkan [Penugasan: kontrol yang ditentukan organisasi]] ketika pelanggaran integritas ditemukan.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-07 (05)	Secara otomatis [Seleksi (satu atau lebih): matikan sistem; restart sistem; menerapkan [Penugasan: kontrol yang ditentukan organisasi]] ketika pelanggaran integritas ditemukan.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
SI-07 (15)	Menerapkan mekanisme kriptografi untuk mengotentikasi komponen perangkat lunak atau firmware berikut sebelum instalasi: [Penugasan: perangkat lunak yang ditentukan organisasi atau komponen firmware].	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-07 (15)	Menerapkan mekanisme kriptografi untuk mengotentikasi komponen perangkat lunak atau firmware berikut sebelum instalasi: [Penugasan: perangkat lunak yang ditentukan organisasi atau komponen firmware].	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk FedRAMP (Bagian Tinggi 2).

Praktik Terbaik Operasional untuk FFIEC

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara domain Alat Penilaian Keamanan Cyber Dewan Pemeriksaan Lembaga Keuangan Federal (FFIEC) dan aturan Config yang dikelola AWS . Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau beberapa

kontrol Alat Penilaian Keamanan Cyber FFIEC. Kontrol Alat Penilaian Keamanan Cyber FFIEC dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D1.G.IT.B.1	Inventarisasi aset organisasi (misalnya , perangkat keras, perangkat lunak, data, dan sistem yang dihosting secara eksternal) dipertaha nkan.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.
D1.G.IT.B.1	Inventarisasi aset organisasi (misalnya , perangkat keras, perangkat lunak, data, dan sistem	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	yang dihosting secara eksternal) dipertaha nkan.		Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.
D1.G.IT.B.1	Inventarisasi aset organisasi (misalnya , perangkat keras, perangkat lunak, data, dan sistem yang dihosting secara eksternal) dipertaha nkan.	ec2- volume-inuse-check	Aturan ini memastika n bahwa volume Amazon Elastic Block Store yang dilampirk an ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentika n, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D1.G.IT.B.1	Inventarisasi aset organisasi (misalnya , perangkat keras, perangkat lunak, data, dan sistem yang dihosting secara eksternal) dipertaha nkan.	terlampir eip	Aturan ini memastika n Elastic IPs dialokasi kan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan. Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D1.rm.rm.b.1	Fungsi manajemen risiko keamanan informasi dan kelangsungan bisnis ada di dalam institusi.	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D1.rm.rm.b.1	Fungsi manajemen risiko keamanan informasi dan kelangsungan bisnis ada di dalam institusi.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D1.rm.rm.b.1	Fungsi manajemen risiko keamanan informasi dan kelangsungan bisnis ada di dalam institusi.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D1.rm.rm.b.1	Fungsi manajemen risiko keamanan informasi dan kelangsungan bisnis ada di dalam institusi.	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D1.rm.rm.b.1	Fungsi manajemen risiko keamanan informasi dan kelangsungan bisnis ada di dalam institusi.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D1.rm.rm.b.1	Fungsi manajemen risiko keamanan informasi dan kelangsungan bisnis ada di dalam institusi.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D1.rm.rm.b.1	Fungsi manajemen risiko keamanan informasi dan kelangsungan bisnis ada di dalam institusi.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D1.rm.rm.b.1	Fungsi manajemen risiko keamanan informasi dan kelangsungan bisnis ada di dalam institusi.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D1.rm.rm.b.1	Fungsi manajemen risiko keamanan informasi dan kelangsungan bisnis ada di dalam institusi.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D1.rm.rm.b.1	Fungsi manajemen risiko keamanan informasi dan kelangsungan bisnis ada di dalam institusi.	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D1.rm.rm.b.1	Fungsi manajemen risiko keamanan informasi dan kelangsungan bisnis ada di dalam institusi.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D1.rm.rm.b.1	Fungsi manajemen risiko keamanan informasi dan kelangsungan bisnis ada di dalam institusi.	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D1.rm.rm.b.1	Fungsi manajemen risiko keamanan informasi dan kelangsungan bisnis ada di dalam institusi.	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D1.rm.rm.b.1	Fungsi manajemen risiko keamanan informasi dan kelangsungan bisnis ada di dalam institusi.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D1.rm.rm.b.1	Fungsi manajemen risiko keamanan informasi dan kelangsungan bisnis ada di dalam institusi.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D1.RM.RA.B.2	Penilaian risiko mengidentifikasi sistem berbasis Internet dan transaksi berisiko tinggi yang menjamin kontrol otentikasi tambahan.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
D1.RM.RA.B.2	Penilaian risiko mengidentifikasi sistem berbasis Internet dan transaksi berisiko tinggi yang menjamin kontrol otentikasi tambahan.	annual-risk-assessment-performed (pemeriksaan proses)	Lakukan penilaian risiko tahunan pada organisasi Anda. Penilaian risiko dapat membantu dalam menentukan kemungkinan dan dampak dari risiko dan/atau kerentanan yang diidentifikasi yang mempengaruhi suatu organisasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D1.tc.tr.b.2	Pelatihan keamanan informasi tahunan mencakup respons insiden, ancaman dunia maya saat ini (misalnya, phishing, phishing tombak, rekayasa sosial, dan keamanan seluler), dan masalah yang muncul.	security-awareness -program-exists (pemeriksaan proses)	Membangun dan memelihara program kesadaran keamanan untuk organisas i Anda. Program kesadaran keamanan mendidik karyawan tentang cara melindungi organisas i mereka dari berbagai pelanggaran atau insiden keamanan.
D2.is.is.b.1	Ancaman keamanan informasi dikumpulkan dan dibagikan dengan karyawan internal yang berlaku.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D2.is.is.b.1	Ancaman keamanan informasi dikumpulkan dan dibagikan dengan karyawan internal yang berlaku.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D2.is.is.b.1	Ancaman keamanan informasi dikumpulkan dan dibagikan dengan karyawan internal yang berlaku.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D2.ma.ma.b.1	Catatan log audit dan log peristiwa keamanan lainnya ditinjau dan disimpan dengan cara yang aman.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
D2.ma.ma.b.1	Catatan log audit dan log peristiwa keamanan lainnya ditinjau dan disimpan dengan cara yang aman.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D2.ma.ma.b.1	Catatan log audit dan log peristiwa keamanan lainnya ditinjau dan disimpan dengan cara yang aman.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D2.ma.ma.b.1	Catatan log audit dan log peristiwa keamanan lainnya ditinjau dan disimpan dengan cara yang aman.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D2.ma.ma.b.1	Catatan log audit dan log peristiwa keamanan lainnya ditinjau dan disimpan dengan cara yang aman.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D2.ma.ma.b.1	Catatan log audit dan log peristiwa keamanan lainnya ditinjau dan disimpan dengan cara yang aman.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
D2.ma.ma.b.1	Catatan log audit dan log peristiwa keamanan lainnya ditinjau dan disimpan dengan cara yang aman.	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D2.ma.ma.b.1	Catatan log audit dan log peristiwa keamanan lainnya ditinjau dan disimpan dengan cara yang aman.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
D2.ma.ma.b.1	Catatan log audit dan log peristiwa keamanan lainnya ditinjau dan disimpan dengan cara yang aman.	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D2.ma.ma.b.1	Catatan log audit dan log peristiwa keamanan lainnya ditinjau dan disimpan dengan cara yang aman.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D2.ma.ma.b.1	Catatan log audit dan log peristiwa keamanan lainnya ditinjau dan disimpan dengan cara yang aman.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D2.ma.ma.b.1	Catatan log audit dan log peristiwa keamanan lainnya ditinjau dan disimpan dengan cara yang aman.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D2.ma.ma.b.1	Catatan log audit dan log peristiwa keamanan lainnya ditinjau dan disimpan dengan cara yang aman.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
D2.ma.ma.b.1	Catatan log audit dan log peristiwa keamanan lainnya ditinjau dan disimpan dengan cara yang aman.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D2.ma.ma.b.2	Log peristiwa komputer digunakan untuk investiga si setelah suatu peristiwa terjadi.	api-gw-execution-l ogging-diaktifkan	Pencatatan API Gateway menampilk an tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
D2.ma.ma.b.2	Log peristiwa komputer digunakan untuk investiga si setelah suatu peristiwa terjadi.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D2.ma.ma.b.2	Log peristiwa komputer digunakan untuk investiga si setelah suatu peristiwa terjadi.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D2.ma.ma.b.2	Log peristiwa komputer digunakan untuk investiga si setelah suatu peristiwa terjadi.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D2.ma.ma.b.2	Log peristiwa komputer digunakan untuk investiga si setelah suatu peristiwa terjadi.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D2.ma.ma.b.2	Log peristiwa komputer digunakan untuk investiga si setelah suatu peristiwa terjadi.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediak an metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinc i untuk permintaa n yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D2.ma.ma.b.2	Log peristiwa komputer digunakan untuk investiga si setelah suatu peristiwa terjadi.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
D2.ma.ma.b.2	Log peristiwa komputer digunakan untuk investiga si setelah suatu peristiwa terjadi.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteks i aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D2.ma.ma.b.2	Log peristiwa komputer digunakan untuk investiga si setelah suatu peristiwa terjadi.	redshift-cluster-c onfiguration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastika n bahwa konfigura si yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberika n informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapka n untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D2.ma.ma.b.2	Log peristiwa komputer digunakan untuk investiga si setelah suatu peristiwa terjadi.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D2.ti.ti.b.1	Lembaga ini termasuk atau berlangganan sumber berbagi informasi ancaman dan kerentanan yang menyediakan informasi tentang ancaman (misalnya, FS-ISAC, AS-CERT).	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D2.ti.ti.b.1	Lembaga ini termasuk atau berlangganan sumber berbagi informasi ancaman dan kerentanan yang menyediakan informasi tentang ancaman (misalnya, FS-ISAC, AS-CERT).	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D2.ti.ti.b.2	Informasi ancaman digunakan untuk memantau ancaman dan kerentanan.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D2.ti.ti.b.2	Informasi ancaman digunakan untuk memantau ancaman dan kerentanan.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D2.ti.ti.b.2	Informasi ancaman digunakan untuk memantau ancaman dan kerentanan.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D2.ti.ti.b.3	Informasi ancaman digunakan untuk meningkatkan manajemen dan pengendalian risiko internal.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D2.ti.ti.b.3	Informasi ancaman digunakan untuk meningkatkan manajemen dan pengendalian risiko internal.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.CC.PM.B.1	Program manajemen tambalan diimplementasikan dan memastikan bahwa tambalan perangkat lunak dan firmware diterapkan tepat waktu.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
D3.CC.PM.B.1	Program manajemen tambalan diimplementasikan dan memastikan bahwa tambalan perangkat lunak dan firmware diterapkan tepat waktu.	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.CC.PM.B.1	Program manajemen tambalan diimplementasikan dan memastikan bahwa tambalan perangkat lunak dan firmware diterapkan tepat waktu.	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relational Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.CC.PM.B.1	Program manajemen tambalan diimplementasikan dan memastikan bahwa tambalan perangkat lunak dan firmware diterapkan tepat waktu.	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.CC.PM.B.3	Laporan manajemen patch ditinjau dan mencerminkan patch keamanan yang hilang.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
D3.CC.PM.B.3	Laporan manajemen patch ditinjau dan mencerminkan patch keamanan yang hilang.	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.CC.PM.B.3	Laporan manajemen patch ditinjau dan mencerminkan patch keamanan yang hilang.	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relational Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.CC.PM.B.3	Laporan manajemen patch ditinjau dan mencerminkan patch keamanan yang hilang.	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.an.b.1	Lembaga ini mampu mendeteksi aktivitas anomali melalui pemantauan di seluruh lingkungan.	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.an.b.1	Lembaga ini mampu mendeteksi aktivitas anomali melalui pemantauan di seluruh lingkungan.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.an.b.1	Lembaga ini mampu mendeteksi aktivitas anomali melalui pemantauan di seluruh lingkungan.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.an.b.2	Transaksi pelanggan yang menghasilkan peringatan aktivitas anomali dipantau dan ditinjau.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.an.b.2	Transaksi pelanggan yang menghasilkan peringatan aktivitas anomali dipantau dan ditinjau.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.an.b.3	Log akses fisik dan/atau logis ditinjau peristiwa berikut.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.an.b.3	Log akses fisik dan/atau logis ditinjau peristiwa berikut.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.an.b.3	Log akses fisik dan/atau logis ditinjau peristiwa berikut.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.an.b.3	Log akses fisik dan/atau logis ditinjau peristiwa berikut.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.an.b.3	Log akses fisik dan/atau logis ditinjau peristiwa berikut.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
D3.dc.an.b.3	Log akses fisik dan/atau logis ditinjau peristiwa berikut.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.an.b.3	Log akses fisik dan/atau logis ditinjau peristiwa berikut.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
D3.dc.an.b.3	Log akses fisik dan/atau logis ditinjau peristiwa berikut.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.an.b.3	Log akses fisik dan/atau logis ditinjau peristiwa berikut.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
D3.dc.an.b.3	Log akses fisik dan/atau logis ditinjau peristiwa berikut.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.an.b.3	Log akses fisik dan/atau logis ditinjau peristiwa berikut.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.an.b.4	Akses ke sistem kritis oleh pihak ketiga dipantau untuk aktivitas yang tidak sah atau tidak biasa	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.an.b.4	Akses ke sistem kritis oleh pihak ketiga dipantau untuk aktivitas yang tidak sah atau tidak biasa	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.an.b.4	Akses ke sistem kritis oleh pihak ketiga dipantau untuk aktivitas yang tidak sah atau tidak biasa	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.an.b.4	Akses ke sistem kritis oleh pihak ketiga dipantau untuk aktivitas yang tidak sah atau tidak biasa	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.an.b.4	Akses ke sistem kritis oleh pihak ketiga dipantau untuk aktivitas yang tidak sah atau tidak biasa	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
D3.dc.an.b.4	Akses ke sistem kritis oleh pihak ketiga dipantau untuk aktivitas yang tidak sah atau tidak biasa	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.an.b.4	Akses ke sistem kritis oleh pihak ketiga dipantau untuk aktivitas yang tidak sah atau tidak biasa	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
D3.dc.an.b.4	Akses ke sistem kritis oleh pihak ketiga dipantau untuk aktivitas yang tidak sah atau tidak biasa	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.an.b.4	Akses ke sistem kritis oleh pihak ketiga dipantau untuk aktivitas yang tidak sah atau tidak biasa	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.an.b.4	Akses ke sistem kritis oleh pihak ketiga dipantau untuk aktivitas yang tidak sah atau tidak biasa	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.an.b.4	Akses ke sistem kritis oleh pihak ketiga dipantau untuk aktivitas yang tidak sah atau tidak biasa	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
D3.dc.an.b.4	Akses ke sistem kritis oleh pihak ketiga dipantau untuk aktivitas yang tidak sah atau tidak biasa	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.an.b.5	Hak istimewa yang ditinggikan dipantau.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
D3.dc.an.b.5	Hak istimewa yang ditinggikan dipantau.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.ev.b.1	Garis dasar aktivitas jaringan normal ditetapkan.	lambda-concurrency-check	Aturan ini memastikan bahwa batas tinggi dan rendah konkurensi fungsi Lambda ditetapkan. Ini dapat membantu dalam mendasarkan jumlah permintaan yang dilayani oleh fungsi Anda pada waktu tertentu.
D3.dc.ev.b.1	Garis dasar aktivitas jaringan normal ditetapkan.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
D3.dc.ev.b.1	Garis dasar aktivitas jaringan normal ditetapkan.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.ev.b.1	Garis dasar aktivitas jaringan normal ditetapkan.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.ev.b.1	Garis dasar aktivitas jaringan normal ditetapkan.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.
D3.dc.ev.b.1	Garis dasar aktivitas jaringan normal ditetapkan.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteks i aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.ev.b.1	Garis dasar aktivitas jaringan normal ditetapkan.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.ev.b.1	Garis dasar aktivitas jaringan normal ditetapkan.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDbEncrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.ev.b.1	Garis dasar aktivitas jaringan normal ditetapkan.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.ev.b.2	Mekanisme (misalnya , peringatan antivirus , peringatan peristiwa log) ada untuk mengingatkan manajemen terhadap potensi serangan.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.ev.b.3	Proses dilakukan untuk memantau keberadaan pengguna, perangkat , koneksi, dan perangkat lunak yang tidak sah.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.ev.b.3	Proses dilakukan untuk memantau keberadaan pengguna, perangkat , koneksi, dan perangkat lunak yang tidak sah.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.ev.b.3	Proses dilakukan untuk memantau keberadaan pengguna, perangkat , koneksi, dan perangkat lunak yang tidak sah.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.ev.b.3	Proses dilakukan untuk memantau keberadaan pengguna, perangkat , koneksi, dan perangkat lunak yang tidak sah.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.th.b.1	Pengujian independen (termasuk pengujian penetrasi dan pemindaian kerentanan) dilakukan sesuai dengan penilaian risiko untuk sistem yang menghadap eksternal dan jaringan internal.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.th.b.1	Pengujian independen (termasuk pengujian penetrasi dan pemindaian kerentanan) dilakukan sesuai dengan penilaian risiko untuk sistem yang menghadap eksternal dan jaringan internal.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.dc.th.b.1	Pengujian independen (termasuk pengujian penetrasi dan pemindaian kerentanan) dilakukan sesuai dengan penilaian risiko untuk sistem yang menghadap eksternal dan jaringan internal.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.1	Akses karyawan diberikan ke sistem dan data rahasia berdasarkan tanggung jawab pekerjaan dan prinsip-prinsip hak istimewa yang paling rendah.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.1	Akses karyawan diberikan ke sistem dan data rahasia berdasarkan tanggung jawab pekerjaan dan prinsip-prinsip hak istimewa yang paling rendah.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.1	Akses karyawan diberikan ke sistem dan data rahasia berdasarkan tanggung jawab pekerjaan dan prinsip-prinsip hak istimewa yang paling rendah.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.1	Akses karyawan diberikan ke sistem dan data rahasia berdasarkan tanggung jawab pekerjaan dan prinsip-prinsip hak istimewa yang paling rendah.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.1	Akses karyawan diberikan ke sistem dan data rahasia berdasarkan tanggung jawab pekerjaan dan prinsip-prinsip hak istimewa yang paling rendah.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.1	Akses karyawan diberikan ke sistem dan data rahasia berdasarkan tanggung jawab pekerjaan dan prinsip-prinsip hak istimewa yang paling rendah.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.
D3.pc.am.b.1	Akses karyawan diberikan ke sistem dan data rahasia berdasarkan tanggung jawab pekerjaan dan prinsip-prinsip hak istimewa yang paling rendah.	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirk an profil instans ke instans Anda dapat membantu pengelola an hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.1	Akses karyawan diberikan ke sistem dan data rahasia berdasarkan tanggung jawab pekerjaan dan prinsip-prinsip hak istimewa yang paling rendah.	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.1	Akses karyawan diberikan ke sistem dan data rahasia berdasarkan tanggung jawab pekerjaan dan prinsip-prinsip hak istimewa yang paling rendah.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.1	Akses karyawan diberikan ke sistem dan data rahasia berdasarkan tanggung jawab pekerjaan dan prinsip-prinsip hak istimewa yang paling rendah.	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
D3.pc.am.b.1	Akses karyawan diberikan ke sistem dan data rahasia berdasarkan tanggung jawab pekerjaan dan prinsip-prinsip hak istimewa yang paling rendah.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.10	Lingkungan produksi dan non-produksi dipisahkan untuk mencegah akses yang tidak sah atau perubahan aset informasi. (*N/A jika tidak ada lingkunga n produksi di institusi atau pihak ketiga lembaga.)	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.10	Lingkungan produksi dan non-produksi dipisahkan untuk mencegah akses yang tidak sah atau perubahan aset informasi. (*N/A jika tidak ada lingkungan produksi di institusi atau pihak ketiga lembaga.)	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.10	Lingkungan produksi dan non-produksi dipisahkan untuk mencegah akses yang tidak sah atau perubahan aset informasi. (*N/A jika tidak ada lingkunga n produksi di institusi atau pihak ketiga lembaga.)	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.10	Lingkungan produksi dan non-produksi dipisahkan untuk mencegah akses yang tidak sah atau perubahan aset informasi. (*N/A jika tidak ada lingkungan produksi di institusi atau pihak ketiga lembaga.)	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.12	Semua kata sandi dienkripsi dalam penyimpanan dan dalam perjalanan.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.12	Semua kata sandi dienkripsi dalam penyimpanan dan dalam perjalanan.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
D3.pc.am.b.12	Semua kata sandi dienkripsi dalam penyimpanan dan dalam perjalanan.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.12	Semua kata sandi dienkripsi dalam penyimpanan dan dalam perjalanan.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
D3.pc.am.b.12	Semua kata sandi dienkripsi dalam penyimpanan dan dalam perjalanan.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.12	Semua kata sandi dienkripsi dalam penyimpanan dan dalam perjalanan.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
D3.pc.am.b.12	Semua kata sandi dienkripsi dalam penyimpanan dan dalam perjalanan.	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.12	Semua kata sandi dienkripsi dalam penyimpanan dan dalam perjalanan.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
D3.pc.am.b.12	Semua kata sandi dienkripsi dalam penyimpanan dan dalam perjalanan.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.12	Semua kata sandi dienkripsi dalam penyimpanan dan dalam perjalanan.	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
D3.pc.am.b.12	Semua kata sandi dienkripsi dalam penyimpanan dan dalam perjalanan.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.12	Semua kata sandi dienkripsi dalam penyimpanan dan dalam perjalanan.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan Applicati on Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
D3.pc.am.b.12	Semua kata sandi dienkripsi dalam penyimpanan dan dalam perjalanan.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.12	Semua kata sandi dienkripsi dalam penyimpanan dan dalam perjalanan.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.12	Semua kata sandi dienkripsi dalam penyimpanan dan dalam perjalanan.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.12	Semua kata sandi dienkripsi dalam penyimpanan dan dalam perjalanan.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
D3.pc.am.b.12	Semua kata sandi dienkripsi dalam penyimpanan dan dalam perjalanan.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.12	Semua kata sandi dienkripsi dalam penyimpanan dan dalam perjalanan.	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
D3.pc.am.b.12	Semua kata sandi dienkripsi dalam penyimpanan dan dalam perjalanan.	s3- default-encryption -kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.13	Data rahasia dienkrips i saat dikirimkan melalui jaringan publik atau tidak tepercaya (misalnya, Internet).	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
D3.pc.am.b.13	Data rahasia dienkrips i saat dikirimkan melalui jaringan publik atau tidak tepercaya (misalnya, Internet).	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan Applicati on Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.13	Data rahasia dienkripsi saat dikirimkan melalui jaringan publik atau tidak tepercaya (misalnya, Internet).	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
D3.pc.am.b.13	Data rahasia dienkripsi saat dikirimkan melalui jaringan publik atau tidak tepercaya (misalnya, Internet).	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.13	Data rahasia dienkrips i saat dikirimkan melalui jaringan publik atau tidak tepercaya (misalnya, Internet).	s3- bucket-ssl-request s-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
D3.pc.am.b.13	Data rahasia dienkrips i saat dikirimkan melalui jaringan publik atau tidak tepercaya (misalnya, Internet).	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.13	Data rahasia dienkrips i saat dikirimkan melalui jaringan publik atau tidak tepercaya (misalnya, Internet).	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.15	Akses jarak jauh ke sistem kritis oleh karyawan, kontraktor, dan pihak ketiga menggunakan koneksi terenkripsi dan otentikasi multifaktor.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.15	Akses jarak jauh ke sistem kritis oleh karyawan, kontraktor, dan pihak ketiga menggunakan koneksi terenkripsi dan otentikasi multifaktor.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.15	Akses jarak jauh ke sistem kritis oleh karyawan, kontraktor, dan pihak ketiga menggunakan koneksi terenkripsi dan otentikasi multifaktor.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.15	Akses jarak jauh ke sistem kritis oleh karyawan, kontraktor, dan pihak ketiga menggunakan koneksi terenkripsi dan otentikasi multifaktor.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.15	Akses jarak jauh ke sistem kritis oleh karyawan, kontraktor, dan pihak ketiga menggunakan koneksi terenkripsi dan otentikasi multifaktor.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
D3.pc.am.b.15	Akses jarak jauh ke sistem kritis oleh karyawan, kontraktor, dan pihak ketiga menggunakan koneksi terenkripsi dan otentikasi multifaktor.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.15	Akses jarak jauh ke sistem kritis oleh karyawan, kontraktor, dan pihak ketiga menggunakan koneksi terenkripsi dan otentikasi multifaktor.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.16	Kontrol administr atif, fisik, atau teknis ada untuk mencegah pengguna tanpa tanggung jawab administratif menginstal perangkat lunak yang tidak sah.	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.16	Kontrol administr atif, fisik, atau teknis ada untuk mencegah pengguna tanpa tanggung jawab administratif menginstal perangkat lunak yang tidak sah.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.16	Kontrol administr atif, fisik, atau teknis ada untuk mencegah pengguna tanpa tanggung jawab administratif menginstal perangkat lunak yang tidak sah.	iam-user-group-membership-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastika n pengguna adalah anggota setidaknya satu grup. Mengizink an pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
D3.pc.am.b.16	Kontrol administr atif, fisik, atau teknis ada untuk mencegah pengguna tanpa tanggung jawab administratif menginstal perangkat lunak yang tidak sah.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.2	Akses karyawan ke sistem dan data rahasia menyediakan pemisahan tugas.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.2	Akses karyawan ke sistem dan data rahasia menyediakan pemisahan tugas.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
D3.pc.am.b.2	Akses karyawan ke sistem dan data rahasia menyediakan pemisahan tugas.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.3	Hak istimewa yang ditinggikan (misalnya , hak administr ator) terbatas dan dikontrol dengan ketat (misalnya, ditugaska n untuk individu, tidak dibagikan, dan memerlukan kontrol kata sandi yang lebih kuat)	root-account-hardw are-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindun gan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.3	Hak istimewa yang ditinggikan (misalnya , hak administr ator) terbatas dan dikontrol dengan ketat (misalnya, ditugaska n untuk individu, tidak dibagikan, dan memerlukan kontrol kata sandi yang lebih kuat)	root-account-mfa-e nabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindun gan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.3	Hak istimewa yang ditinggikan (misalnya , hak administr ator) terbatas dan dikontrol dengan ketat (misalnya, ditugaska n untuk individu, tidak dibagikan, dan memerlukan kontrol kata sandi yang lebih kuat).	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.3	Hak istimewa yang ditinggikan (misalnya , hak administr ator) terbatas dan dikontrol dengan ketat (misalnya, ditugaska n untuk individu, tidak dibagikan, dan memerlukan kontrol kata sandi yang lebih kuat)	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.3	Hak istimewa yang ditinggikan (misalnya, hak administrator) terbatas dan dikontrol dengan ketat (misalnya, ditugaskan untuk individu, tidak dibagikan, dan memerlukan kontrol kata sandi yang lebih kuat)	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.3	Hak istimewa yang ditinggikan (misalnya , hak administr ator) terbatas dan dikontrol dengan ketat (misalnya, ditugaska n untuk individu, tidak dibagikan, dan memerlukan kontrol kata sandi yang lebih kuat)	iam-policy-no-stat ements-with-full-a ccess	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.6	Identifikasi dan otentikasi diperlukan dan dikelola untuk akses ke sistem, aplikasi, dan perangkat keras.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.6	Identifikasi dan otentikasi diperlukan dan dikelola untuk akses ke sistem, aplikasi, dan perangkat keras.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.6	Identifikasi dan otentikasi diperlukan dan dikelola untuk akses ke sistem, aplikasi, dan perangkat keras.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.6	Identifikasi dan otentikasi diperlukan dan dikelola untuk akses ke sistem, aplikasi, dan perangkat keras.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.6	Identifikasi dan otentikasi diperlukan dan dikelola untuk akses ke sistem, aplikasi, dan perangkat keras.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.6	Identifikasi dan otentikasi diperlukan dan dikelola untuk akses ke sistem, aplikasi, dan perangkat keras.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.6	Identifikasi dan otentikasi diperlukan dan dikelola untuk akses ke sistem, aplikasi, dan perangkat keras.	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.6	Identifikasi dan otentikasi diperlukan dan dikelola untuk akses ke sistem, aplikasi, dan perangkat keras.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.6	Identifikasi dan otentikasi diperlukan dan dikelola untuk akses ke sistem, aplikasi, dan perangkat keras.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.6	Identifikasi dan otentikasi diperlukan dan dikelola untuk akses ke sistem, aplikasi, dan perangkat keras.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.
D3.pc.am.b.6	Identifikasi dan otentikasi diperlukan dan dikelola untuk akses ke sistem, aplikasi, dan perangkat keras.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.7	Kontrol akses mencakup kompleksitas kata sandi dan batasan untuk upaya dan penggunaan kembali kata sandi.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.am.b.8	Semua kata sandi default dan akun default yang tidak perlu diubah sebelum implementasi sistem.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindungi nya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.1	Alat pertahanan perimeter jaringan (misalnya, router perbatasan dan firewall) digunakan.	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositor i data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.PC.IM.B.2	Sistem yang diakses dari Internet atau oleh pihak eksternal dilindungi oleh firewall atau perangkat serupa lainnya.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.PC.IM.B.2	Sistem yang diakses dari Internet atau oleh pihak eksternal dilindungi oleh firewall atau perangkat serupa lainnya.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.PC.IM.B.2	Sistem yang diakses dari Internet atau oleh pihak eksternal dilindungi oleh firewall atau perangkat serupa lainnya.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.PC.IM.B.2	Sistem yang diakses dari Internet atau oleh pihak eksternal dilindungi oleh firewall atau perangkat serupa lainnya.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.PC.IM.B.2	Sistem yang diakses dari Internet atau oleh pihak eksternal dilindungi oleh firewall atau perangkat serupa lainnya.	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindungi nya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.PC.IM.B.2	Sistem yang diakses dari Internet atau oleh pihak eksternal dilindungi oleh firewall atau perangkat serupa lainnya.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.PC.IM.B.3	Semua port dipantau.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
D3.PC.IM.B.3	Semua port dipantau.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.PC.IM.B.3	Semua port dipantau.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
D3.PC.IM.B.3	Semua port dipantau.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.PC.IM.B.3	Semua port dipantau.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.PC.IM.B.3	Semua port dipantau.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.5	Konfigurasi sistem (untuk server, desktop, router, dll.) mengikuti standar industri dan diberlaku kan	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.5	Konfigurasi sistem (untuk server, desktop, router, dll.) mengikuti standar industri dan diberlaku kan	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.5	Konfigurasi sistem (untuk server, desktop, router, dll.) mengikuti standar industri dan diberlaku kan	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.PC.IM.B.6	Pelabuhan, fungsi, protokol, dan layanan dilarang jika tidak lagi diperlukan untuk tujuan bisnis.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.PC.IM.B.6	Pelabuhan, fungsi, protokol, dan layanan dilarang jika tidak lagi diperlukan untuk tujuan bisnis.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.PC.IM.B.6	Pelabuhan, fungsi, protokol, dan layanan dilarang jika tidak lagi diperlukan untuk tujuan bisnis.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.PC.IM.B.6	Pelabuhan, fungsi, protokol, dan layanan dilarang jika tidak lagi diperlukan untuk tujuan bisnis.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.7	Akses untuk membuat perubahan pada konfigurasi sistem (termasuk mesin virtual dan hypervisor) dikendalikan dan dipantau.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.7	Akses untuk membuat perubahan pada konfigurasi sistem (termasuk mesin virtual dan hyperviso r) dikendalikan dan dipantau.	iam-user-no-policies-periksa	Aturan ini memastika n kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapka n hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.7	Akses untuk membuat perubahan pada konfigurasi sistem (termasuk mesin virtual dan hyperviso r) dikendalikan dan dipantau.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.7	Akses untuk membuat perubahan pada konfigurasi sistem (termasuk mesin virtual dan hypervisor) dikendalikan dan dipantau.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.7	Akses untuk membuat perubahan pada konfigurasi sistem (termasuk mesin virtual dan hyperviso r) dikendalikan dan dipantau.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
D3.pc.im.b.7	Akses untuk membuat perubahan pada konfigurasi sistem (termasuk mesin virtual dan hyperviso r) dikendalikan dan dipantau.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.im.b.7	Akses untuk membuat perubahan pada konfigurasi sistem (termasuk mesin virtual dan hypervisor) dikendalikan dan dipantau.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
D3.pc.se.b.1	Pengembang yang bekerja untuk institusi mengikuti praktik pengkodean program yang aman, sebagai bagian dari siklus hidup pengembangan sistem (SDLC), yang memenuhi standar industri.	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild. Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D3.pc.se.b.1	Pengembang yang bekerja untuk institusi mengikuti praktik pengkodean program yang aman, sebagai bagian dari siklus hidup pengembangan sistem (SDLC), yang memenuhi standar industri.	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredensyal masuk dalam lingkungan proyek Codebuild . AWS Gunakan OAuth alih-alih token akses pribadi atau kredensyal masuk untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D4.C.Co.B.2	Lembaga memastikan bahwa koneksi pihak ketiga diotorisasi.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D4.C.Co.B.2	Lembaga memastikan bahwa koneksi pihak ketiga diotorisasi.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D4.C.Co.B.2	Lembaga memastikan bahwa koneksi pihak ketiga diotorisasi.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D4.C.Co.B.2	Lembaga memastikan bahwa koneksi pihak ketiga diotorisasi.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.dr.de.b.1	Parameter peringatan ditetapkan untuk mendeteksi insiden keamanan informasi yang meminta tindakan mitigasi.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.dr.de.b.1	Parameter peringatan ditetapkan untuk mendeteksi insiden keamanan informasi yang meminta tindakan mitigasi.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.dr.de.b.1	Parameter peringatan ditetapkan untuk mendeteksi insiden keamanan informasi yang meminta tindakan mitigasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
D5.dr.de.b.2	Laporan kinerja sistem berisi informasi yang dapat digunakan sebagai indikator risiko untuk mendeteksi insiden keamanan informasi	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.dr.de.b.2	Laporan kinerja sistem berisi informasi yang dapat digunakan sebagai indikator risiko untuk mendeteksi insiden keamanan informasi	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
D5.dr.de.b.3	Alat dan proses tersedia untuk mendeteksi, memperingatkan, dan memicu program respons insiden.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.dr.de.b.3	Alat dan proses tersedia untuk mendeteksi, memperingatkan, dan memicu program respons insiden.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.
D5.dr.de.b.3	Alat dan proses tersedia untuk mendeteksi, memperingatkan, dan memicu program respons insiden.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteks i aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.dr.de.b.3	Alat dan proses tersedia untuk mendeteksi, memperingatkan, dan memicu program respons insiden.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.dr.de.b.3	Alat dan proses tersedia untuk mendeteksi, memperingatkan, dan memicu program respons insiden.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.dr.de.b.3	Alat dan proses tersedia untuk mendeteksi, memperingatkan, dan memicu program respons insiden.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.dr.de.b.3	Alat dan proses tersedia untuk mendeteksi, memperingatkan, dan memicu program respons insiden.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.dr.de.b.3	Alat dan proses tersedia untuk mendeteksi, memperingatkan, dan memicu program respons insiden.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
D5.dr.de.b.3	Alat dan proses tersedia untuk mendeteksi, memperingatkan, dan memicu program respons insiden.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.dr.de.b.3	Alat dan proses tersedia untuk mendeteksi, memperingatkan, dan memicu program respons insiden.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.dr.de.b.3	Alat dan proses tersedia untuk mendeteksi, memperingatkan, dan memicu program respons insiden.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.dr.de.b.3	Alat dan proses tersedia untuk mendeteksi, memperingatkan, dan memicu program respons insiden.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.er.ESB.4	Insiden diklasifikasikan, dicatat dan dilacak.	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.
D5.ir.pl.b.1	Lembaga ini telah mendokumentasikan bagaimana ia akan bereaksi dan menanggapi insiden cyber.	response-plan-exists-maintained (pemeriksaan proses)	Memastikan rencana respons insiden dibuat, dipelihara, dan didistribusikan kepada personel yang bertanggung jawab.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.ir.pl.b.6	Lembaga ini berencana untuk menggunakan kelangsungan bisnis, pemulihan bencana, dan program cadangan data untuk memulihkan operasi setelah insiden.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.ir.pl.b.6	Lembaga ini berencana untuk menggunakan kelangsungan bisnis, pemulihan bencana, dan program cadangan data untuk memulihkan operasi setelah insiden.	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.ir.pl.b.6	Lembaga ini berencana untuk menggunakan kelangsungan bisnis, pemulihan bencana, dan program cadangan data untuk memulihkan operasi setelah insiden.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.ir.pl.b.6	Lembaga ini berencana untuk menggunakan kelangsungan bisnis, pemulihan bencana, dan program cadangan data untuk memulihkan operasi setelah insiden.	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.ir.pl.b.6	Lembaga ini berencana untuk menggunakan kelangsungan bisnis, pemulihan bencana, dan program cadangan data untuk memulihkan operasi setelah insiden.	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
D5.ir.pl.b.6	Lembaga ini berencana untuk menggunakan kelangsungan bisnis, pemulihan bencana, dan program cadangan data untuk memulihkan operasi setelah insiden.	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.ir.pl.b.6	Lembaga ini berencana untuk menggunakan kelangsungan bisnis, pemulihan bencana, dan program cadangan data untuk memulihkan operasi setelah insiden.	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.ir.pl.b.6	Lembaga ini berencana untuk menggunakan kelangsungan bisnis, pemulihan bencana, dan program cadangan data untuk memulihkan operasi setelah insiden.	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.ir.pl.b.6	Lembaga ini berencana untuk menggunakan kelangsungan bisnis, pemulihan bencana, dan program cadangan data untuk memulihkan operasi setelah insiden.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.ir.pl.b.6	Lembaga ini berencana untuk menggunakan kelangsungan bisnis, pemulihan bencana, dan program cadangan data untuk memulihkan operasi setelah insiden.	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.ir.pl.b.6	Lembaga ini berencana untuk menggunakan kelangsungan bisnis, pemulihan bencana, dan program cadangan data untuk memulihkan operasi setelah insiden.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.ir.pl.b.6	Lembaga ini berencana untuk menggunakan kelangsungan bisnis, pemulihan bencana, dan program cadangan data untuk memulihkan operasi setelah insiden.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.ir.pl.b.6	Lembaga ini berencana untuk menggunakan kelangsungan bisnis, pemulihan bencana, dan program cadangan data untuk memulihkan operasi setelah insiden.	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.ir.pl.b.6	Lembaga ini berencana untuk menggunakan kelangsungan bisnis, pemulihan bencana, dan program cadangan data untuk memulihkan operasi setelah insiden.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.ir.pl.b.6	Lembaga ini berencana untuk menggunakan kelangsungan bisnis, pemulihan bencana, dan program cadangan data untuk memulihkan operasi setelah insiden.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.ir.pl.b.6	Lembaga ini berencana untuk menggunakan kelangsungan bisnis, pemulihan bencana, dan program cadangan data untuk memulihkan operasi setelah insiden.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.ir.pl.b.6	Lembaga ini berencana untuk menggunakan kelangsungan bisnis, pemulihan bencana, dan program cadangan data untuk memulihkan operasi setelah insiden.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.ir.pl.b.6	Lembaga ini berencana untuk menggunakan kelangsungan bisnis, pemulihan bencana, dan program cadangan data untuk memulihkan operasi setelah insiden.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.
D5.ir.pl.b.6	Lembaga ini berencana untuk menggunakan kelangsungan bisnis, pemulihan bencana, dan program cadangan data untuk memulihkan operasi setelah insiden.	lambda-concurrency-check	Aturan ini memastika n bahwa batas tinggi dan rendah konkurens i fungsi Lambda ditetapkan. Ini dapat membantu dalam mendasarkan jumlah permintaan yang dilayani oleh fungsi Anda pada waktu tertentu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.ir.pl.b.6	Lembaga ini berencana untuk menggunakan kelangsungan bisnis, pemulihan bencana, dan program cadangan data untuk memulihkan operasi setelah insiden.	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.ir.pl.b.6	Lembaga ini berencana untuk menggunakan kelangsungan bisnis, pemulihan bencana, dan program cadangan data untuk memulihkan operasi setelah insiden.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.ir.pl.b.6	Lembaga ini berencana untuk menggunakan kelangsungan bisnis, pemulihan bencana, dan program cadangan data untuk memulihkan operasi setelah insiden.	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D5.ir.pl.b.6	Lembaga ini berencana untuk menggunakan kelangsungan bisnis, pemulihan bencana, dan program cadangan data untuk memulihkan operasi setelah insiden.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk FFIEC.

Praktik Terbaik Operasional untuk Katalog Kriteria Kepatuhan Komputasi Awan Jerman (C5)

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS

Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara Katalog Kriteria Kepatuhan Komputasi Awan Jerman (C5) dan aturan AWS Config terkelola. Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau beberapa kontrol C5 Jerman. Kontrol C5 Jerman dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	AWS Aturan Config	Bimbingan
COS-01	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.
COS-01	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan

ID Kontrol	AWS Aturan Config	Bimbingan
		tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindung inya dari serangan berbahaya
COS-01	waf-regional-rule-not-kosong	Pastikan AWS WAF Anda memiliki aturan yang tidak kosong. Aturan tanpa kondisi dapat mengakibatkan perilaku yang tidak diinginkan.
COS-01	waf-regional-rulegroup-not-kosong	Pastikan AWS WAF Anda memiliki grup aturan yang tidak kosong. Grup aturan yang kosong dapat mengakiba tkan perilaku yang tidak diinginkan.
COS-01	waf-regional-webacl-not-kos ong	Web ACL yang dilampirk an ke AWS WAF dapat berisi kumpulan aturan dan kelompok aturan untuk memeriksa dan mengontro l permintaan web. Jika ACL Web kosong, lalu lintas web lewat tanpa terdeteksi atau ditindaklanjuti oleh WAF.

ID Kontrol	AWS Aturan Config	Bimbingan
COS-01	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
COS-03	alb-waf-enabled	Pastikan AWS WAF diaktifka n pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.
COS-03	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
COS-03	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
COS-03	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
COS-03	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	AWS Aturan Config	Bimbingan
COS-03	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearc h Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
COS-03	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearc h Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	AWS Aturan Config	Bimbingan
COS-03	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
COS-03	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkin kan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabk an akses tidak sah ke sumber daya VPC Amazon.
COS-03	lambda-function-public-acce ss-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses publik. Akses publik berpotens i menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	AWS Aturan Config	Bimbingan
COS-03	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyarat an untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.
COS-03	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
COS-03	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
COS-03	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
COS-03	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,338 9,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
COS-03	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	AWS Aturan Config	Bimbingan
COS-03	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
COS-03	sagemaker-notebook-no-direc t-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
COS-03	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .
COS-03	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	AWS Aturan Config	Bimbingan
COS-03	alb-http-drop-invalid-header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
COS-05	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredensyal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
COS-05	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensyal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
COS-05	root-account-hardware-mfa-d iaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan ekstra untuk kredensyal masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
COS-05	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifka n untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensyal masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
COS-05	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
COS-05	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
COS-05	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
COS-05	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
COS-05	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
COS-05	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,338 9,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
COS-05	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	AWS Aturan Config	Bimbingan
COS-05	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .
COS-05	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	AWS Aturan Config	Bimbingan
MENANG-02	alb-http-to-https-pengalihan-periksa	Untuk membantu melindung i data dalam perjalanan, pastikan bahwa Applicati on Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
MENANG-02	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifika t SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	AWS Aturan Config	Bimbingan
MENANG-02	elb-predefined-security-policy-ssl-periksa	Untuk membantu melindung i data dalam perjalanan, pastikan bahwa pendengar SSL Classic Elastic Load Balancing Anda menggunak an kebijakan keamanan yang telah ditentukan sebelumny a. Elastic Load Balancing menyediakan konfigurasi negosiasi SSL yang telah ditentukan sebelumny a yang digunakan untuk negosiasi SSL ketika koneksi dibuat antara klien dan penyeimbang beban Anda. Konfigurasi negosiasi SSL memberikan kompatibilitas dengan berbagai klien dan menggunakan algoritma kriptografi berkekuatan tinggi. Aturan ini mengharus kan Anda menetapkan kebijakan keamanan yang telah ditentukan untuk pendengar SSL Anda. Kebijakan keamanan default adalah: ELBSecurity Policy-TLS-1-2-2017-0. Nilai aktual harus mencerminkan kebijakan organisasi Anda

ID Kontrol	AWS Aturan Config	Bimbingan
MENANG-02	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindung i data dalam perjalanan, pastikan HTTPS diaktifka n untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
MENANG-02	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
MENANG-02	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
MENANG-02	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerluka n enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
MENANG-02	s3- bucket-ssl-requests-only	Untuk membantu melindung i data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerluka n permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
MENANG-02	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
MENANG-03	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
MENANG-03	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
MENANG-03	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
MENANG-03	kinesis-stream-encrypted	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
MENANG-03	secretsmanager-using-cmk	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
MENANG-03	dynamodb-table-encrypted-km s	Pastikan enkripsi diaktifka n untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
MENANG-03	ebs-snapshot-public-restora ble-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihka n secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
MENANG-03	ec2- ebs-encryption-by-default	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
MENANG-03	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
MENANG-03	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
MENANG-03	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
MENANG-03	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
MENANG-03	rds-snapshot-encrypted	Pastikan enkripsi diaktifka n untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
MENANG-03	codebuild-project-artifact-encryption	Untuk membantu melindung i data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk AWS CodeBuild artefak Anda.
MENANG-03	rds-storage-encrypted	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
MENANG-03	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
MENANG-03	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
MENANG-03	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
MENANG-03	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
MENANG-03	sns-encrypted-kms	Untuk membantu melindung i data saat istirahat, pastikan topik Amazon Simple Notificat ion Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
MENANG-04	cmk-backing-key-rotation-di aktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.
DEV-07	cloud-trail-cloud-watch-logs- diaktifkan	Gunakan Amazon CloudWatc h untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaa n AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	AWS Aturan Config	Bimbingan
DEV-07	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi terperinci tentang proyek build Anda.
DEV-07	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	AWS Aturan Config	Bimbingan
DEV-07	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penol akan dengan merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilka n, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
DEV-07	cloudtrail-s3-dataevents-di aktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	AWS Aturan Config	Bimbingan
DEV-07	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimk an file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
IDM-01	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaima na ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
IDM-01	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribus i kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertah ankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	AWS Aturan Config	Bimbingan
IDM-01	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
IDM-01	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.
IDM-01	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
IDM-01	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredensyal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
IDM-01	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentif ikasi, Anda harus menonakti fkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
IDM-01	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensyal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
IDM-01	root-account-hardware-mfa-d iaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan ekstra untuk kredensyal masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
IDM-01	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifka n untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensyal masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
IDM-01	secretsmanager-rotation-ena bled-check	Aturan ini memastikan AWS rahasia Secrets Manager mengaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotens i mengurangi dampak bisnis jika rahasia itu dikomprom ikan.
IDM-01	secretsmanager-scheduled-ro tation-success-periksa	Aturan ini memastikan bahwa AWS rahasia Secrets Manager telah berhasil diputar sesuai dengan jadwal rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode di mana rahasia aktif, dan berpotensi mengurangi dampak bisnis jika dikomprom ikan.

ID Kontrol	AWS Aturan Config	Bimbingan
IDM-01	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.
IDM-01	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	AWS Aturan Config	Bimbingan
IDM-01	codebuild-project-envvar-awscred-periksa	Pastikan kredensyal otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild. Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.
IDM-01	ecs-containers-nonprivileged	Untuk membantu menerapkan prinsip hak istimewa paling rendah, definisi tugas Amazon Elastic Container Service (Amazon ECS) seharusnya tidak mengaktifkan hak istimewa yang ditinggikan. Ketika parameter ini benar, wadah diberikan hak istimewa yang ditinggikan pada instance wadah host (mirip dengan pengguna root).

ID Kontrol	AWS Aturan Config	Bimbingan
IDM-01	ecs-containers-readonly-access	Mengaktifkan akses baca saja ke wadah Amazon Elastic Container Service (ECS) dapat membantu mematuhi prinsip hak istimewa yang paling rendah. Opsi ini dapat mengurangi vektor serangan karena sistem file instance container tidak dapat dimodifikasi kecuali jika memiliki izin baca-tulis eksplisit.
IDM-01	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.
IDM-01	efs-access-point-enforce-root-direktori	Menegakkan direktori root untuk jalur akses Amazon Elastic File System (Amazon EFS) membantu membatasi akses data dengan memastikan bahwa pengguna jalur akses hanya dapat menjangkau file dari subdirektori yang ditentukan.

ID Kontrol	AWS Aturan Config	Bimbingan
IDM-01	efs-access-point-enforce-identitas pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan penegakan pengguna diaktifkan untuk Amazon Elastic File System (Amazon EFS) Anda. Saat diaktifkan, Amazon EFS menggantikan pengguna dan grup klien NFS IDs dengan identitas yang dikonfigurasi pada titik akses untuk semua operasi sistem file dan hanya memberikan akses ke identitas pengguna yang diberlakukan ini.
IDM-01	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
IDM-01	opensearch-access-control-enabled	Pastikan kontrol akses berbutir halus diaktifkan di domain Layanan Amazon OpenSearch Anda. Kontrol akses berbutir halus menyediakan mekanisme otorisasi yang disempurnakan untuk mencapai akses yang paling tidak memiliki hak istimewa ke domain Layanan Amazon. OpenSearch Ini memungkinkan kontrol akses berbasis peran ke domain, serta indeks, dokumen, dan keamanan tingkat lapangan, dukungan untuk dasbor OpenSearch Layanan multi-tenancy, dan otentikasi dasar HTTP untuk Layanan dan Kibana. OpenSearch

ID Kontrol	AWS Aturan Config	Bimbingan
IDM-01	rds-instance-iam-authentication-diaktifkan	Pastikan autentikasi AWS Identity and Access Management (IAM) diaktifkan pada instans Amazon Relational Database Service (Amazon RDS) untuk mengontrol akses ke sistem dan aset. Ini memberlakukan lalu lintas jaringan ke dan dari database yang akan dienkripsi menggunakan Secure Sockets Layer (SSL). Anda tidak diharuskan untuk menyimpan kredensi pengguna dalam database, karena otentikasi dikelola secara eksternal.
IDM-01	s3- bucket-acl-prohibited	Aturan ini memeriksa untuk melihat apakah Daftar Kontrol Akses (ACLs) digunakan untuk kontrol akses di Bucket Amazon S3. ACLs adalah mekanisme kontrol akses lama untuk bucket Amazon S3 yang AWS mendahului Identity and Access Management (IAM). Sebagai gantinya ACLs, ini adalah praktik terbaik untuk menggunakan kebijakan IAM atau kebijakan bucket S3 untuk mengelola akses ke bucket S3 Anda dengan lebih mudah.

ID Kontrol	AWS Aturan Config	Bimbingan
IDM-03	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentif ikasi, Anda harus menonakti fkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
IDM-03	secretsmanager-secret-unused	Jika kredensyal yang tidak digunakan ada di AWS Secrets Manager, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini memungkinkan Anda untuk menetapkan nilai ke unusedForDays (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
IDM-08	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
MENANG-01	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
IDM-09	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredensyal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
IDM-09	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensyal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
IDM-09	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensyal masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
IDM-09	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensyal masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-01	clb-multiple-az	Elastic Load Balancing (ELB) secara otomatis mendistribusikan lalu lintas masuk Anda di beberapa target, seperti EC2 instans, kontainer, dan alamat IP, di zona ketersediaan. Untuk memastikan ketersediaan tinggi, pastikan ELB Anda telah mendaftarkan instans dari beberapa Availability Zone.
OPS-01	elbv2-multiple-az	Elastic Load Balancing (ELB) secara otomatis mendistribusikan lalu lintas masuk Anda di beberapa target, seperti EC2 instans, kontainer, dan alamat IP, di zona ketersediaan. Untuk memastikan ketersediaan tinggi, pastikan ELB Anda telah mendaftarkan instans dari beberapa Availability Zone.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-01	lambda-vpc-multi-az-periksa	Jika fungsi AWS Lambda Anda dikonfigurasi untuk terhubung ke virtual private cloud (VPC) di akun Anda, gunakan fungsi AWS Lambda di setidaknya dua Availabil ity Zone yang berbeda untuk memastikan bahwa fungsi Anda tersedia untuk memproses peristiwa jika terjadi gangguan layanan di satu zona.
OPS-01	rds-cluster-multi-az-diaktifkan	Cluster Amazon Relational Database Service (Amazon RDS) harus mengaktifkan replikasi Multi-AZ untuk membantu ketersediaan data yang disimpan. Setiap Availability Zone berjalan pada infrastruktur independe n yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-01	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independe n yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-01	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.
OPS-01	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-01	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-02	clb-multiple-az	Elastic Load Balancing (ELB) secara otomatis mendistribusikan lalu lintas masuk Anda di beberapa target, seperti EC2 instans, kontainer, dan alamat IP, di zona ketersediaan. Untuk memastikan ketersediaan tinggi, pastikan ELB Anda telah mendaftarkan instans dari beberapa Availability Zone.
OPS-02	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-02	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.
OPS-02	elbv2-multiple-az	Elastic Load Balancing (ELB) secara otomatis mendistribusikan lalu lintas masuk Anda di beberapa target, seperti EC2 instans, kontainer, dan alamat IP, di zona ketersediaan. Untuk memastikan ketersediaan tinggi, pastikan ELB Anda telah mendaftarkan instans dari beberapa Availability Zone.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-02	lambda-vpc-multi-az-periksa	Jika fungsi AWS Lambda Anda dikonfigurasi untuk terhubung ke virtual private cloud (VPC) di akun Anda, gunakan fungsi AWS Lambda di setidaknya dua Availabil ity Zone yang berbeda untuk memastikan bahwa fungsi Anda tersedia untuk memproses peristiwa jika terjadi gangguan layanan di satu zona.
OPS-02	rds-cluster-multi-az-diaktifkan	Cluster Amazon Relational Database Service (Amazon RDS) harus mengaktifkan replikasi Multi-AZ untuk membantu ketersediaan data yang disimpan. Setiap Availability Zone berjalan pada infrastruktur independe n yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-02	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independe n yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-02	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.
OPS-02	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-02	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-07	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-07	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-07	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.
OPS-07	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan cadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.
OPS-07	opensearch-data-node-fault-toleransi	Amazon OpenSearch Service (OpenSearch Service) memerlukan setidaknya tiga node data untuk ketersedi aan tinggi dan toleransi kesalahan. Menyebarkan domain OpenSearch Layanan dengan setidaknya tiga node data memastikan operasi klaster jika node gagal.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-07	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-07	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.
OPS-07	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-07	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
OPS-07	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-07	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
OPS-07	elasticache-redis-cluster-a utomatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCac he membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentuka n oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-07	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
OPS-07	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relational Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-07	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.
OPS-12	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-12	s3- lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigu rasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihkan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).
OPS-13	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-13	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-13	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-14	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.
OPS-14	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-14	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.
OPS-14	s3- lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigu rasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihkan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).
OPS-15	api-gw-execution-logging-di aktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-15	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
OPS-15	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi terperinci tentang proyek build Anda.
OPS-15	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-15	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.
OPS-15	opensearch-audit-logging-enabled	Pastikan pencatatan audit diaktifkan di domain OpenSearch Layanan Amazon Anda. Pencatatan audit memungkinkan Anda melacak aktivitas pengguna di OpenSearch domain Anda, termasuk keberhasilan dan kegagalan otentikasi, permintaan, perubahan indeks OpenSearch, dan kueri penelusuran yang masuk.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-15	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
OPS-15	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
OPS-15	redshift-audit-logging-enabled	Untuk menangkap informasi tentang koneksi dan aktivitas pengguna di klaster Amazon Redshift, pastikan pencatatan audit diaktifkan.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-15	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.
OPS-15	vpc-flow-logs-enabled	Log aliran VPC menyediak an catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-15	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
OPS-15	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-15	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
OPS-15	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-15	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimk an file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
OPS-22	ecr-private-image-scanning-diaktifkan	Pemindaian gambar Amazon Elastic Container Repository (ECR) membantu mengident ifikasi kerentanan perangkat lunak dalam gambar kontainer Anda. Mengaktif kan pemindaian gambar pada repositori ECR menambahk an lapisan verifikasi untuk integritas dan keamanan gambar yang disimpan.
PSS-05	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredensyal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
PSS-05	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensyal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
PSS-05	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensyal masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
PSS-05	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensyal masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
PSS-07	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

Templat

Template tersedia di GitHub: Katalog Kriteria Kepatuhan Komputasi Awan Jerman (C5).

Praktik Terbaik Operasional untuk Gramm Leach Bliley Act (GLBA)

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini menyediakan contoh pemetaan antara aturan Gramm-Leach-Bliley Act (GLBA) dan managed AWS Config. Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan berhubungan dengan satu atau beberapa kontrol GLBA. Kontrol GLBA dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	keuangan yang tunduk pada yurisdiksinya yang berkaitan dengan pengamanan administratif, teknis, dan fisik		akses diperlukan untuk akun tersebut.
GLBA-SEC.501 (b)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksinya yang berkaitan dengan pengamanan administratif, teknis, dan fisik	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksinya yang berkaitan dengan pengamanan administratif, teknis, dan fisik	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksinya yang berkaitan dengan pengamanan administratif, teknis, dan fisik	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksinya yang berkaitan dengan pengamanan administratif, teknis, dan fisik	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksinya yang berkaitan dengan pengamanan administratif, teknis, dan fisik	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksinya yang berkaitan dengan pengamanan administratif, teknis, dan fisik	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
GLBA-SEC.501 (b)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksinya yang berkaitan dengan pengamanan administratif, teknis, dan fisik	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksinya yang berkaitan dengan pengamanan administratif, teknis, dan fisik	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigurasi ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksinya yang berkaitan dengan pengamanan administratif, teknis, dan fisik	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
GLBA-SEC.501 (b)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksinya yang berkaitan dengan pengamanan administratif, teknis, dan fisik	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksinya yang berkaitan dengan pengamanan administratif, teknis, dan fisik	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksinya yang berkaitan dengan pengamanan administratif, teknis, dan fisik	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksinya yang berkaitan dengan pengamanan administratif, teknis, dan fisik	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
GLBA-SEC.501 (b)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksinya yang berkaitan dengan pengamanan administratif, teknis, dan fisik	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksinya yang berkaitan dengan pengamanan administratif, teknis, dan fisik	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
GLBA-SEC.501 (b)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksinya yang berkaitan dengan pengamanan administratif, teknis, dan fisik	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksinya yang berkaitan dengan pengamanan administratif, teknis, dan fisik	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
GLBA-SEC.501 (b)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksinya yang berkaitan dengan pengamanan administratif, teknis, dan fisik	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksinya yang berkaitan dengan pengamanan administratif, teknis, dan fisik	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksinya yang berkaitan dengan pengamanan administratif, teknis, dan fisik	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam grup keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksinya yang berkaitan dengan pengamanan administratif, teknis, dan fisik	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (1)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (1) untuk menjamin keamanan dan kerahasiaan catatan dan informasi pelanggan;	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (1)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (1) untuk menjamin keamanan dan kerahasiaan catatan dan informasi pelanggan;	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (1)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (1) untuk menjamin keamanan dan kerahasiaan catatan dan informasi pelanggan;	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (1)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (1) untuk menjamin keamanan dan kerahasiaan catatan dan informasi pelanggan;	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (1)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (1) untuk menjamin keamanan dan kerahasiaan catatan dan informasi pelanggan;	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (1)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (1) untuk menjamin keamanan dan kerahasiaan catatan dan informasi pelanggan;	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (1)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (1) untuk menjamin keamanan dan kerahasiaan catatan dan informasi pelanggan;	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (1)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (1) untuk menjamin keamanan dan kerahasiaan catatan dan informasi pelanggan;	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (1)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (1) untuk menjamin keamanan dan kerahasiaan catatan dan informasi pelanggan;	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (1)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (1) untuk menjamin keamanan dan kerahasiaan catatan dan informasi pelanggan;	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (1)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (1) untuk menjamin keamanan dan kerahasiaan catatan dan informasi pelanggan;	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (1)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (1) untuk menjamin keamanan dan kerahasiaan catatan dan informasi pelanggan;	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (1)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (1) untuk menjamin keamanan dan kerahasiaan catatan dan informasi pelanggan;	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (1)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (1) untuk menjamin keamanan dan kerahasiaan catatan dan informasi pelanggan;	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (1)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (1) untuk menjamin keamanan dan kerahasiaan catatan dan informasi pelanggan;	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (1)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (1) untuk menjamin keamanan dan kerahasiaan catatan dan informasi pelanggan;	s3- default-encryption -kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (1)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (1) untuk menjamin keamanan dan kerahasiaan catatan dan informasi pelanggan;	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (1)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (1) untuk menjamin keamanan dan kerahasiaan catatan dan informasi pelanggan;	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (1)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (1) untuk menjamin keamanan dan kerahasiaan catatan dan informasi pelanggan;	codebuild-project-s3-log-terenkripsi	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk AWS CodeBuild log Anda yang disimpan di Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (1)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (1) untuk menjamin keamanan dan kerahasiaan catatan dan informasi pelanggan;	codebuild-project-artifact-encryption	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk AWS CodeBuild artefak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (1)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (1) untuk menjamin keamanan dan kerahasiaan catatan dan informasi pelanggan;	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (1)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (1) untuk menjamin keamanan dan kerahasiaan catatan dan informasi pelanggan;	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (1)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (1) untuk menjamin keamanan dan kerahasiaan catatan dan informasi pelanggan;	kinesis-stream-encrypted	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (2)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksinya terkait dengan pengamanan administratif, teknis, dan fisik (2) untuk melindungi terhadap ancaman atau bahaya yang diantisipasi terhadap keamanan atau integritas catatan tersebut; dan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (2)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksinya terkait dengan pengamanan administratif, teknis, dan fisik (2) untuk melindungi terhadap ancaman atau bahaya yang diantisipasi terhadap keamanan atau integritas catatan tersebut; dan	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (3)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (3) untuk melindungi terhadap akses yang tidak sah ke atau penggunaan catatan atau informasi tersebut yang dapat mengakibatkan kerugian besar atau ketidaknyamanan bagi pelanggan mana pun.	secretsmanager-rotation-enabled-check	Aturan ini memastikan AWS rahasia Secrets Manager mengaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (3)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (3) untuk melindungi terhadap akses yang tidak sah ke atau penggunaan catatan atau informasi tersebut yang dapat mengakibatkan kerugian besar atau ketidaknyamanan bagi pelanggan mana pun.	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (3)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (3) untuk melindungi terhadap akses yang tidak sah ke atau penggunaan catatan atau informasi tersebut yang dapat mengakibatkan kerugian besar atau ketidaknyamanan bagi pelanggan mana pun.	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (3)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (3) untuk melindungi terhadap akses yang tidak sah ke atau penggunaan catatan atau informasi tersebut yang dapat mengakibatkan kerugian besar atau ketidaknyamanan bagi pelanggan mana pun.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (3)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (3) untuk melindungi terhadap akses yang tidak sah ke atau penggunaan catatan atau informasi tersebut yang dapat mengakibatkan kerugian besar atau ketidaknyamanan bagi pelanggan mana pun.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (3)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (3) untuk melindungi terhadap akses yang tidak sah ke atau penggunaan catatan atau informasi tersebut yang dapat mengakibatkan kerugian besar atau ketidaknyamanan bagi pelanggan mana pun.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (3)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (3) untuk melindungi terhadap akses yang tidak sah ke atau penggunaan catatan atau informasi tersebut yang dapat mengakibatkan kerugian besar atau ketidaknyamanan bagi pelanggan mana pun.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (3)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (3) untuk melindungi terhadap akses yang tidak sah ke atau penggunaan catatan atau informasi tersebut yang dapat mengakibatkan kerugian besar atau ketidaknyamanan bagi pelanggan mana pun.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (3)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (3) untuk melindungi terhadap akses yang tidak sah ke atau penggunaan catatan atau informasi tersebut yang dapat mengakibatkan kerugian besar atau ketidaknyamanan bagi pelanggan mana pun.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsageUsia (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (3)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (3) untuk melindungi terhadap akses yang tidak sah ke atau penggunaan catatan atau informasi tersebut yang dapat mengakibatkan kerugian besar atau ketidaknyamanan bagi pelanggan mana pun.	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (3)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (3) untuk melindungi terhadap akses yang tidak sah ke atau penggunaan catatan atau informasi tersebut yang dapat mengakibatkan kerugian besar atau ketidaknyamanan bagi pelanggan mana pun.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (3)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (3) untuk melindungi terhadap akses yang tidak sah ke atau penggunaan catatan atau informasi tersebut yang dapat mengakibatkan kerugian besar atau ketidaknyamanan bagi pelanggan mana pun.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (3)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (3) untuk melindungi terhadap akses yang tidak sah ke atau penggunaan catatan atau informasi tersebut yang dapat mengakibatkan kerugian besar atau ketidaknyamanan bagi pelanggan mana pun.	opensearch-access-control-enabled	Pastikan kontrol akses berbutir halus diaktifkan di domain Layanan Amazon OpenSearch Anda. Kontrol akses berbutir halus menyediakan mekanisme otorisasi yang disempurnakan untuk mencapai akses yang paling tidak memiliki hak istimewa ke domain Layanan Amazon. OpenSearch Ini memungkinkan kontrol akses berbasis peran ke domain, serta indeks, dokumen, dan keamanan tingkat lapangan, dukungan untuk dasbor OpenSearch Layanan multi-tenancy, dan otentikasi dasar HTTP untuk Layanan dan Kibana. OpenSearch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (3)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (3) untuk melindungi terhadap akses yang tidak sah ke atau penggunaan catatan atau informasi tersebut yang dapat mengakibatkan kerugian besar atau ketidaknyamanan bagi pelanggan mana pun.	ecs-containers-readonly-access	Mengaktifkan akses baca saja ke kontainer Amazon Elastic Container Service (ECS) dapat membantu mematuhi prinsip hak istimewa yang paling rendah. Opsi ini dapat mengurangi vektor serangan karena sistem file instance container tidak dapat dimodifikasi kecuali jika memiliki izin baca-tulis eksplisit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (3)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (3) untuk melindungi terhadap akses yang tidak sah ke atau penggunaan catatan atau informasi tersebut yang dapat mengakibatkan kerugian besar atau ketidaknyamanan bagi pelanggan mana pun.	efs-access-point-enforce-root-direktori	Menegakkan direktori root untuk jalur akses Amazon Elastic File System (Amazon EFS) membantu membatasi akses data dengan memastikan bahwa pengguna jalur akses hanya dapat menjangkau file dari subdirektori yang ditentukan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
GLBA-SEC.501 (b) (3)	Sebagai kelanjutan dari kebijakan dalam ayat (a), setiap lembaga atau otoritas yang dijelaskan dalam pasal 505 (a) harus menetapkan standar yang sesuai untuk lembaga keuangan yang tunduk pada yurisdiksi mereka yang berkaitan dengan perlindungan administratif, teknis, dan fisik (3) untuk melindungi terhadap akses yang tidak sah ke atau penggunaan catatan atau informasi tersebut yang dapat mengakibatkan kerugian besar atau ketidaknyamanan bagi pelanggan mana pun.	efs-access-point-enforce-identitas pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan penegakan pengguna diaktifkan untuk Amazon Elastic File System (Amazon EFS) Anda. Saat diaktifkan, Amazon EFS mengganti kan pengguna dan grup klien NFS IDs dengan identitas yang dikonfigurasi pada titik akses untuk semua operasi sistem file dan hanya memberikan akses ke identitas pengguna yang diberlakukan ini.

Templat

Template ini tersedia di GitHub: Praktik Terbaik Operasional untuk Gramm Leach Bliley Act (GLBA).

Praktik Terbaik Operasional untuk GxP EU Annex 11

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS

Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini menyediakan contoh pemetaan antara GxP EU Annex 11 dan aturan Config terkelola AWS . Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau beberapa kontrol GxP EU Annex 11. Kontrol GxP EU Annex 11 dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1. Manajemen Risiko	Manajemen risiko harus diterapkan sepanjang siklus hidup sistem komputerisasi dengan mempertimbangkan keselamatan pasien, integritas data, dan kualitas produk. Sebagai bagian dari sistem manajemen risiko, keputusan tentang tingkat validasi dan kontrol integritas data harus didasarkan pada penilaian risiko yang dibenarkan dan didokumentasikan dari sistem komputeri sasi.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
1. Manajemen Risiko	Manajemen risiko harus diterapkan sepanjang siklus	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi,

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	hidup sistem komputerisasi dengan mempertimbangkan keselamatan pasien, integritas data, dan kualitas produk. Sebagai bagian dari sistem manajemen risiko, keputusan tentang tingkat validasi dan kontrol integritas data harus didasarkan pada penilaian risiko yang dibenarkan dan didokumentasikan dari sistem komputeri sasi.		perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.2. Validasi - Kontrol Perubahan Dokumentasi	Dokumentasi validasi harus mencakup catatan kontrol perubahan (jika berlaku) dan laporan tentang penyimpan gan yang diamati selama proses validasi.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.3. Validasi - Persediaan	Daftar terbaru dari semua sistem yang relevan dan fungsiona litas GMP (inventar is) mereka harus tersedia. Untuk sistem kritis, deskripsi sistem terkini yang merinci pengaturan fisik dan logis, aliran data dan antarmuka dengan sistem atau proses lain, prasyarat perangkat keras dan perangkat lunak apa pun, dan langkah-l angkah keamanan harus tersedia.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.3. Validasi - Persediaan	Daftar terbaru dari semua sistem yang relevan dan fungsionalitas GMP (inventaris) mereka harus tersedia. Untuk sistem kritis, deskripsi sistem terkini yang merinci pengaturan fisik dan logis, aliran data dan antarmuka dengan sistem atau proses lain, prasyarat perangkat keras dan perangkat lunak apa pun, dan langkah-langkah keamanan harus tersedia.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.3. Validasi - Persediaan	Daftar terbaru dari semua sistem yang relevan dan fungsiona litas GMP (inventar is) mereka harus tersedia. Untuk sistem kritis, deskripsi sistem terkini yang merinci pengaturan fisik dan logis, aliran data dan antarmuka dengan sistem atau proses lain, prasyarat perangkat keras dan perangkat lunak apa pun, dan langkah-l angkah keamanan harus tersedia.	ec2- security-group-attached-to -eni-peri odik	Untuk membantu mengelola inventari s aset Anda, aturan ini memeriksa apakah grup keamanan dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) atau ke elastic network interface. Jika grup keamanan Anda tidak melekat pada jenis sumber daya ini, mereka mungkin tidak digunakan dan tidak lagi diperlukan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.3. Validasi - Persediaan	Daftar terbaru dari semua sistem yang relevan dan fungsiona litas GMP (inventar is) mereka harus tersedia. Untuk sistem kritis, deskripsi sistem terkini yang merinci pengaturan fisik dan logis, aliran data dan antarmuka dengan sistem atau proses lain, prasyarat perangkat keras dan perangkat lunak apa pun, dan langkah-l angkah keamanan harus tersedia.	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.3. Validasi - Persediaan	Daftar terbaru dari semua sistem yang relevan dan fungsionalitas GMP (inventaris) mereka harus tersedia. Untuk sistem kritis, deskripsi sistem terkini yang merinci pengaturan fisik dan logis, aliran data dan antarmuka dengan sistem atau proses lain, prasyarat perangkat keras dan perangkat lunak apa pun, dan langkah-langkah keamanan harus tersedia.	terlampir eip	Aturan ini memastikan Elastic IPs dialokasikan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan. Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.3. Validasi - Persediaan	Daftar terbaru dari semua sistem yang relevan dan fungsionalitas GMP (inventaris) mereka harus tersedia. Untuk sistem kritis, deskripsi sistem terkini yang merinci pengaturan fisik dan logis, aliran data dan antarmuka dengan sistem atau proses lain, prasyarat perangkat keras dan perangkat lunak apa pun, dan langkah-langkah keamanan harus tersedia.	vpc-network-acl-unused-periksa	Aturan ini memastikan bahwa daftar kontrol akses jaringan Amazon Virtual Private Cloud (VPC) sedang digunakan. Pemantauan untuk daftar kontrol akses jaringan yang tidak digunakan dapat membantu inventaris dan pengelolaan lingkungan Anda yang akurat.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.8. Validasi - Transfer Data	Jika data ditransfer ke format atau sistem data lain, validasi harus mencakup pemeriksaan bahwa data tidak diubah dalam nilai dan/atau makna selama proses migrasi ini.	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.8. Validasi - Transfer Data	Jika data ditransfer ke format atau sistem data lain, validasi harus mencakup pemeriksaan bahwa data tidak diubah dalam nilai dan/atau makna selama proses migrasi ini.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.8. Validasi - Transfer Data	Jika data ditransfer ke format atau sistem data lain, validasi harus mencakup pemeriksaan bahwa data tidak diubah dalam nilai dan/atau makna selama proses migrasi ini.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
4.8. Validasi - Transfer Data	Jika data ditransfer ke format atau sistem data lain, validasi harus mencakup pemeriksaan bahwa data tidak diubah dalam nilai dan/atau makna selama proses migrasi ini.	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.8. Validasi - Transfer Data	Jika data ditransfer ke format atau sistem data lain, validasi harus mencakup pemeriksaan bahwa data tidak diubah dalam nilai dan/atau makna selama proses migrasi ini.	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.8. Validasi - Transfer Data	Jika data ditransfer ke format atau sistem data lain, validasi harus mencakup pemeriksaan bahwa data tidak diubah dalam nilai dan/atau makna selama proses migrasi ini.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.8. Validasi - Transfer Data	Jika data ditransfer ke format atau sistem data lain, validasi harus mencakup pemeriksaan bahwa data tidak diubah dalam nilai dan/atau makna selama proses migrasi ini.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.8. Validasi - Transfer Data	Jika data ditransfer ke format atau sistem data lain, validasi harus mencakup pemeriksaan bahwa data tidak diubah dalam nilai dan/atau makna selama proses migrasi ini.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.8. Validasi - Transfer Data	Jika data ditransfer ke format atau sistem data lain, validasi harus mencakup pemeriksaan bahwa data tidak diubah dalam nilai dan/atau makna selama proses migrasi ini.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.8. Validasi - Transfer Data	Jika data ditransfer ke format atau sistem data lain, validasi harus mencakup pemeriksaan bahwa data tidak diubah dalam nilai dan/atau makna selama proses migrasi ini.	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.8. Validasi - Transfer Data	Jika data ditransfer ke format atau sistem data lain, validasi harus mencakup pemeriksaan bahwa data tidak diubah dalam nilai dan/atau makna selama proses migrasi ini.	ebs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.8. Validasi - Transfer Data	Jika data ditransfer ke format atau sistem data lain, validasi harus mencakup pemeriksaan bahwa data tidak diubah dalam nilai dan/atau makna selama proses migrasi ini.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.8. Validasi - Transfer Data	Jika data ditransfer ke format atau sistem data lain, validasi harus mencakup pemeriksaan bahwa data tidak diubah dalam nilai dan/atau makna selama proses migrasi ini.	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.8. Validasi - Transfer Data	Jika data ditransfer ke format atau sistem data lain, validasi harus mencakup pemeriksaan bahwa data tidak diubah dalam nilai dan/atau makna selama proses migrasi ini.	efs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.8. Validasi - Transfer Data	Jika data ditransfer ke format atau sistem data lain, validasi harus mencakup pemeriksaan bahwa data tidak diubah dalam nilai dan/atau makna selama proses migrasi ini.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.8. Validasi - Transfer Data	Jika data ditransfer ke format atau sistem data lain, validasi harus mencakup pemeriksaan bahwa data tidak diubah dalam nilai dan/atau makna selama proses migrasi ini.	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.8. Validasi - Transfer Data	Jika data ditransfer ke format atau sistem data lain, validasi harus mencakup pemeriksaan bahwa data tidak diubah dalam nilai dan/atau makna selama proses migrasi ini.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.8. Validasi - Transfer Data	Jika data ditransfer ke format atau sistem data lain, validasi harus mencakup pemeriksaan bahwa data tidak diubah dalam nilai dan/atau makna selama proses migrasi ini.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.8. Validasi - Transfer Data	Jika data ditransfer ke format atau sistem data lain, validasi harus mencakup pemeriksaan bahwa data tidak diubah dalam nilai dan/atau makna selama proses migrasi ini.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.8. Validasi - Transfer Data	Jika data ditransfer ke format atau sistem data lain, validasi harus mencakup pemeriksaan bahwa data tidak diubah dalam nilai dan/atau makna selama proses migrasi ini.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Data	Sistem terkomputerisasi yang bertukar data secara elektronik dengan sistem lain harus mencakup pemeriksaan bawaan yang sesuai untuk entri dan pemrosesan data yang benar dan aman, untuk meminimalkan risiko.	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Data	Sistem terkomputerisasi yang bertukar data secara elektronik dengan sistem lain harus mencakup pemeriksaan bawaan yang sesuai untuk entri dan pemrosesan data yang benar dan aman, untuk meminimalkan risiko.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Data	Sistem terkomputerisasi yang bertukar data secara elektronik dengan sistem lain harus mencakup pemeriksaan bawaan yang sesuai untuk entri dan pemrosesan data yang benar dan aman, untuk meminimalkan risiko.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
5. Data	Sistem terkomputerisasi yang bertukar data secara elektronik dengan sistem lain harus mencakup pemeriksaan bawaan yang sesuai untuk entri dan pemrosesan data yang benar dan aman, untuk meminimalkan risiko.	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Data	Sistem terkomputerisasi yang bertukar data secara elektronik dengan sistem lain harus mencakup pemeriksaan bawaan yang sesuai untuk entri dan pemrosesan data yang benar dan aman, untuk meminimalkan risiko.	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Data	Sistem terkomputerisasi yang bertukar data secara elektronik dengan sistem lain harus mencakup pemeriksaan bawaan yang sesuai untuk entri dan pemrosesan data yang benar dan aman, untuk meminimalkan risiko.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Data	Sistem terkomputerisasi yang bertukar data secara elektronik dengan sistem lain harus mencakup pemeriksaan bawaan yang sesuai untuk entri dan pemrosesan data yang benar dan aman, untuk meminimalkan risiko.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Data	Sistem terkomputerisasi yang bertukar data secara elektronik dengan sistem lain harus mencakup pemeriksaan bawaan yang sesuai untuk entri dan pemrosesan data yang benar dan aman, untuk meminimalkan risiko.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Data	Sistem terkomputerisasi yang bertukar data secara elektronik dengan sistem lain harus mencakup pemeriksaan bawaan yang sesuai untuk entri dan pemrosesan data yang benar dan aman, untuk meminimalkan risiko.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Data	Sistem terkomputerisasi yang bertukar data secara elektronik dengan sistem lain harus mencakup pemeriksaan bawaan yang sesuai untuk entri dan pemrosesan data yang benar dan aman, untuk meminimalkan risiko.	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Data	Sistem terkomputerisasi yang bertukar data secara elektronik dengan sistem lain harus mencakup pemeriksaan bawaan yang sesuai untuk entri dan pemrosesan data yang benar dan aman, untuk meminimalkan risiko.	ebs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Data	Sistem terkomputerisasi yang bertukar data secara elektronik dengan sistem lain harus mencakup pemeriksaan bawaan yang sesuai untuk entri dan pemrosesan data yang benar dan aman, untuk meminimalkan risiko.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Data	Sistem terkomputerisasi yang bertukar data secara elektronik dengan sistem lain harus mencakup pemeriksaan bawaan yang sesuai untuk entri dan pemrosesan data yang benar dan aman, untuk meminimalkan risiko.	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Data	Sistem terkomputerisasi yang bertukar data secara elektronik dengan sistem lain harus mencakup pemeriksaan bawaan yang sesuai untuk entri dan pemrosesan data yang benar dan aman, untuk meminimalkan risiko.	efs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Data	Sistem terkomputerisasi yang bertukar data secara elektronik dengan sistem lain harus mencakup pemeriksaan bawaan yang sesuai untuk entri dan pemrosesan data yang benar dan aman, untuk meminimalkan risiko.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Data	Sistem terkomputerisasi yang bertukar data secara elektronik dengan sistem lain harus mencakup pemeriksaan bawaan yang sesuai untuk entri dan pemrosesan data yang benar dan aman, untuk meminimalkan risiko.	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Data	Sistem terkomputerisasi yang bertukar data secara elektronik dengan sistem lain harus mencakup pemeriksaan bawaan yang sesuai untuk entri dan pemrosesan data yang benar dan aman, untuk meminimalkan risiko.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relational Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Data	Sistem terkomputerisasi yang bertukar data secara elektronik dengan sistem lain harus mencakup pemeriksaan bawaan yang sesuai untuk entri dan pemrosesan data yang benar dan aman, untuk meminimalkan risiko.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Data	Sistem terkomputerisasi yang bertukar data secara elektronik dengan sistem lain harus mencakup pemeriksaan bawaan yang sesuai untuk entri dan pemrosesan data yang benar dan aman, untuk meminimalkan risiko.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Data	Sistem terkomputerisasi yang bertukar data secara elektronik dengan sistem lain harus mencakup pemeriksaan bawaan yang sesuai untuk entri dan pemrosesan data yang benar dan aman, untuk meminimalkan risiko.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1. Penyimpanan Data - Perlindungan Kerusakan	Data harus diamankan dengan cara fisik dan elektronik terhadap kerusakan. Data yang disimpan harus diperiksa untuk aksesibilitas, keterbacaan, dan akurasi. Akses ke data harus dipastikan selama periode retensi.	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
7.1. Penyimpanan Data - Perlindungan Kerusakan	Data harus diamankan dengan cara fisik dan elektronik terhadap kerusakan. Data yang disimpan harus diperiksa untuk aksesibilitas, keterbacaan, dan akurasi. Akses ke data harus dipastikan selama periode retensi.	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1. Penyimpanan Data - Perlindungan Kerusakan	Data harus diamankan dengan cara fisik dan elektronik terhadap kerusakan. Data yang disimpan harus diperiksa untuk aksesibilitas, keterbacaan, dan akurasi. Akses ke data harus dipastikan selama periode retensi.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
7.1. Penyimpanan Data - Perlindungan Kerusakan	Data harus diamankan dengan cara fisik dan elektronik terhadap kerusakan. Data yang disimpan harus diperiksa untuk aksesibilitas, keterbacaan, dan akurasi. Akses ke data harus dipastikan selama periode retensi.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1. Penyimpanan Data - Perlindungan Kerusakan	Data harus diamankan dengan cara fisik dan elektronik terhadap kerusakan. Data yang disimpan harus diperiksa untuk aksesibilitas, keterbacaan, dan akurasi. Akses ke data harus dipastikan selama periode retensi.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1. Penyimpanan Data - Perlindungan Kerusakan	Data harus diamankan dengan cara fisik dan elektronik terhadap kerusakan. Data yang disimpan harus diperiksa untuk aksesibilitas, keterbacaan, dan akurasi. Akses ke data harus dipastikan selama periode retensi.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.
7.1. Penyimpanan Data - Perlindungan Kerusakan	Data harus diamankan dengan cara fisik dan elektronik terhadap kerusakan. Data yang disimpan harus diperiksa untuk aksesibilitas, keterbacaan, dan akurasi. Akses ke data harus dipastikan selama periode retensi.	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1. Penyimpanan Data - Perlindungan Kerusakan	Data harus diamankan dengan cara fisik dan elektronik terhadap kerusakan. Data yang disimpan harus diperiksa untuk aksesibilitas, keterbacaan, dan akurasi. Akses ke data harus dipastikan selama periode retensi.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1. Penyimpanan Data - Perlindungan Kerusakan	Data harus diamankan dengan cara fisik dan elektronik terhadap kerusakan. Data yang disimpan harus diperiksa untuk aksesibilitas, keterbacaan, dan akurasi. Akses ke data harus dipastikan selama periode retensi.	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.
7.1. Penyimpanan Data - Perlindungan Kerusakan	Data harus diamankan dengan cara fisik dan elektronik terhadap kerusakan. Data yang disimpan harus diperiksa untuk aksesibilitas, keterbacaan, dan akurasi. Akses ke data harus dipastikan selama periode retensi.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1. Penyimpanan Data - Perlindungan Kerusakan	Data harus diamankan dengan cara fisik dan elektronik terhadap kerusakan. Data yang disimpan harus diperiksa untuk aksesibilitas, keterbacaan, dan akurasi. Akses ke data harus dipastikan selama periode retensi.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1. Penyimpanan Data - Perlindungan Kerusakan	Data harus diamankan dengan cara fisik dan elektronik terhadap kerusakan. Data yang disimpan harus diperiksa untuk aksesibilitas, keterbacaan, dan akurasi. Akses ke data harus dipastikan selama periode retensi.	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1. Penyimpanan Data - Perlindungan Kerusakan	Data harus diamankan dengan cara fisik dan elektronik terhadap kerusakan. Data yang disimpan harus diperiksa untuk aksesibilitas, keterbacaan, dan akurasi. Akses ke data harus dipastikan selama periode retensi.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.
7.1. Penyimpanan Data - Perlindungan Kerusakan	Data harus diamankan dengan cara fisik dan elektronik terhadap kerusakan. Data yang disimpan harus diperiksa untuk aksesibilitas, keterbacaan, dan akurasi. Akses ke data harus dipastikan selama periode retensi.	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1. Penyimpanan Data - Perlindungan Kerusakan	Data harus diamankan dengan cara fisik dan elektronik terhadap kerusakan. Data yang disimpan harus diperiksa untuk aksesibilitas, keterbacaan, dan akurasi. Akses ke data harus dipastikan selama periode retensi.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1. Penyimpanan Data - Perlindungan Kerusakan	Data harus diamankan dengan cara fisik dan elektronik terhadap kerusakan. Data yang disimpan harus diperiksa untuk aksesibilitas, keterbacaan, dan akurasi. Akses ke data harus dipastikan selama periode retensi.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relational Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1. Penyimpanan Data - Perlindungan Kerusakan	Data harus diamankan dengan cara fisik dan elektronik terhadap kerusakan. Data yang disimpan harus diperiksa untuk aksesibilitas, keterbacaan, dan akurasi. Akses ke data harus dipastikan selama periode retensi.	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
7.1. Penyimpanan Data - Perlindungan Kerusakan	Data harus diamankan dengan cara fisik dan elektronik terhadap kerusakan. Data yang disimpan harus diperiksa untuk aksesibilitas, keterbacaan, dan akurasi. Akses ke data harus dipastikan selama periode retensi.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1. Penyimpanan Data - Perlindungan Kerusakan	Data harus diamankan dengan cara fisik dan elektronik terhadap kerusakan. Data yang disimpan harus diperiksa untuk aksesibilitas, keterbacaan, dan akurasi. Akses ke data harus dipastikan selama periode retensi.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1. Penyimpanan Data - Perlindungan Kerusakan	Data harus diamankan dengan cara fisik dan elektronik terhadap kerusakan. Data yang disimpan harus diperiksa untuk aksesibilitas, keterbacaan, dan akurasi. Akses ke data harus dipastikan selama periode retensi.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDbEncrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1. Penyimpanan Data - Perlindungan Kerusakan	Data harus diamankan dengan cara fisik dan elektronik terhadap kerusakan. Data yang disimpan harus diperiksa untuk aksesibilitas, keterbacaan, dan akurasi. Akses ke data harus dipastikan selama periode retensi.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.
7.1. Penyimpanan Data - Perlindungan Kerusakan	Data harus diamankan dengan cara fisik dan elektronik terhadap kerusakan. Data yang disimpan harus diperiksa untuk aksesibilitas, keterbacaan, dan akurasi. Akses ke data harus dipastikan selama periode retensi.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1. Penyimpanan Data - Perlindungan Kerusakan	Data harus diamankan dengan cara fisik dan elektronik terhadap kerusakan. Data yang disimpan harus diperiksa untuk aksesibilitas, keterbacaan, dan akurasi. Akses ke data harus dipastikan selama periode retensi.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1. Penyimpanan Data - Perlindungan Kerusakan	Data harus diamankan dengan cara fisik dan elektronik terhadap kerusakan. Data yang disimpan harus diperiksa untuk aksesibilitas, keterbacaan, dan akurasi. Akses ke data harus dipastikan selama periode retensi.	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
7.1. Penyimpanan Data - Perlindungan Kerusakan	Data harus diamankan dengan cara fisik dan elektronik terhadap kerusakan. Data yang disimpan harus diperiksa untuk aksesibilitas, keterbacaan, dan akurasi. Akses ke data harus dipastikan selama periode retensi.	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1. Penyimpanan Data - Perlindungan Kerusakan	Data harus diamankan dengan cara fisik dan elektronik terhadap kerusakan. Data yang disimpan harus diperiksa untuk aksesibilitas, keterbacaan, dan akurasi. Akses ke data harus dipastikan selama periode retensi.	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1. Penyimpanan Data - Perlindungan Kerusakan	Data harus diamankan dengan cara fisik dan elektronik terhadap kerusakan. Data yang disimpan harus diperiksa untuk aksesibilitas, keterbacaan, dan akurasi. Akses ke data harus dipastikan selama periode retensi.	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2. Penyimpanan Data - Cadangan	Pencadangan reguler dari semua data yang relevan harus dilakukan. Integrita s dan akurasi data cadangan dan kemampuan untuk mengembalikan data harus diperiksa selama validasi dan dipantau secara berkala.	aurora-resources-p rotected-by-rencana cadangan	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2. Penyimpanan Data - Cadangan	Pencadangan reguler dari semua data yang relevan harus dilakukan. Integrita s dan akurasi data cadangan dan kemampuan untuk mengembalikan data harus diperiksa selama validasi dan dipantau secara berkala.	backup-plan-min-fr equency-and-min-re tention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkin kan Anda untuk mengatur parameter requiredFrequencyV alue (Config default: 1), (requiredR etentionDaysConfig default: 35) dan (requiredFrequencyU nit Config default: days). Nilai aktual harus mencerminkan persyaratan organisas i Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2. Penyimpanan Data - Cadangan	Pencadangan reguler dari semua data yang relevan harus dilakukan. Integrita s dan akurasi data cadangan dan kemampuan untuk mengembalikan data harus diperiksa selama validasi dan dipantau secara berkala.	backup-recovery-po int-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
7.2. Penyimpanan Data - Cadangan	Pencadangan reguler dari semua data yang relevan harus dilakukan. Integrita s dan akurasi data cadangan dan kemampuan untuk mengembalikan data harus diperiksa selama validasi dan dipantau secara berkala.	backup-recovery-po int-manual-penghap usan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapus an titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapus an titik pemulihan dapat membantu mencegah penghapus an yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2. Penyimpanan Data - Cadangan	Pencadangan reguler dari semua data yang relevan harus dilakukan. Integrita s dan akurasi data cadangan dan kemampuan untuk mengembalikan data harus diperiksa selama validasi dan dipantau secara berkala.	backup-recovery-po int-minimum-pemeri ksaan retensi	Untuk membantu proses pencadang an data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkin kan Anda untuk mengatur parameter requiredRetentionD ays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisas i Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2. Penyimpanan Data - Cadangan	Pencadangan reguler dari semua data yang relevan harus dilakukan. Integrita s dan akurasi data cadangan dan kemampuan untuk mengembalikan data harus diperiksa selama validasi dan dipantau secara berkala.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2. Penyimpanan Data - Cadangan	Pencadangan reguler dari semua data yang relevan harus dilakukan. Integrita s dan akurasi data cadangan dan kemampuan untuk mengembalikan data harus diperiksa selama validasi dan dipantau secara berkala.	dynamodb-in-backup-plan	Untuk membantu proses pencadang an data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2. Penyimpanan Data - Cadangan	Pencadangan reguler dari semua data yang relevan harus dilakukan. Integrita s dan akurasi data cadangan dan kemampuan untuk mengembalikan data harus diperiksa selama validasi dan dipantau secara berkala.	dynamodb-pitr-enab led	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertah ankan cadangan dengan memastika n bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2. Penyimpanan Data - Cadangan	Pencadangan reguler dari semua data yang relevan harus dilakukan. Integrita s dan akurasi data cadangan dan kemampuan untuk mengembalikan data harus diperiksa selama validasi dan dipantau secara berkala.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2. Penyimpanan Data - Cadangan	Pencadangan reguler dari semua data yang relevan harus dilakukan. Integrita s dan akurasi data cadangan dan kemampuan untuk mengembalikan data harus diperiksa selama validasi dan dipantau secara berkala.	ebs-optimized-inst ance	Instans yang dioptimal kan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimal kan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2. Penyimpanan Data - Cadangan	Pencadangan reguler dari semua data yang relevan harus dilakukan. Integrita s dan akurasi data cadangan dan kemampuan untuk mengembalikan data harus diperiksa selama validasi dan dipantau secara berkala.	ebs-resources-prot ected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2. Penyimpanan Data - Cadangan	Pencadangan reguler dari semua data yang relevan harus dilakukan. Integrita s dan akurasi data cadangan dan kemampuan untuk mengembalikan data harus diperiksa selama validasi dan dipantau secara berkala.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2. Penyimpanan Data - Cadangan	Pencadangan reguler dari semua data yang relevan harus dilakukan. Integrita s dan akurasi data cadangan dan kemampuan untuk mengembalikan data harus diperiksa selama validasi dan dipantau secara berkala.	efs-in-backup-plan	Untuk membantu proses pencadang an data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2. Penyimpanan Data - Cadangan	Pencadangan reguler dari semua data yang relevan harus dilakukan. Integrita s dan akurasi data cadangan dan kemampuan untuk mengembalikan data harus diperiksa selama validasi dan dipantau secara berkala.	efs-resources-prot ected-by-rencana cadangan	Untuk membantu proses pencadang an data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2. Penyimpanan Data - Cadangan	Pencadangan reguler dari semua data yang relevan harus dilakukan. Integrita s dan akurasi data cadangan dan kemampuan untuk mengembalikan data harus diperiksa selama validasi dan dipantau secara berkala.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2. Penyimpanan Data - Cadangan	Pencadangan reguler dari semua data yang relevan harus dilakukan. Integrita s dan akurasi data cadangan dan kemampuan untuk mengembalikan data harus diperiksa selama validasi dan dipantau secara berkala.	fsx-resources-prot ected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2. Penyimpanan Data - Cadangan	Pencadangan reguler dari semua data yang relevan harus dilakukan. Integrita s dan akurasi data cadangan dan kemampuan untuk mengembalikan data harus diperiksa selama validasi dan dipantau secara berkala.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2. Penyimpanan Data - Cadangan	Pencadangan reguler dari semua data yang relevan harus dilakukan. Integrita s dan akurasi data cadangan dan kemampuan untuk mengembalikan data harus diperiksa selama validasi dan dipantau secara berkala.	redshift-backup-en abled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifka n untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2. Penyimpanan Data - Cadangan	Pencadangan reguler dari semua data yang relevan harus dilakukan. Integrita s dan akurasi data cadangan dan kemampuan untuk mengembalikan data harus diperiksa selama validasi dan dipantau secara berkala.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2. Penyimpanan Data - Cadangan	Pencadangan reguler dari semua data yang relevan harus dilakukan. Integrita s dan akurasi data cadangan dan kemampuan untuk mengembalikan data harus diperiksa selama validasi dan dipantau secara berkala.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
9. Jejak Audit	Pertimbangan harus diberikan, berdasark an penilaian risiko, untuk membangun ke dalam sistem pembuatan catatan semua perubahan dan penghapus an yang relevan dengan GMP (sistem yang dihasilkan “jejak audit”). Untuk perubahan atau penghapusan data yang relevan dengan GMP, alasannya harus didokumen tasikan. Jejak audit harus tersedia dan dapat dikonversi ke bentuk yang dapat dipahami secara umum dan ditinjau secara teratur.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteks i aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10. Manajemen Perubahan dan Konfigurasi	Setiap perubahan pada sistem komputerisasi termasuk konfigurasi sistem hanya boleh dilakukan secara terkontrol sesuai dengan prosedur yang ditentukan.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10. Manajemen Perubahan dan Konfigurasi	Setiap perubahan pada sistem komputerisasi termasuk konfigurasi sistem hanya boleh dilakukan secara terkontrol sesuai dengan prosedur yang ditentukan.	rds-cluster-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10. Manajemen Perubahan dan Konfigurasi	Setiap perubahan pada sistem komputerisasi termasuk konfigurasi sistem hanya boleh dilakukan secara terkontrol sesuai dengan prosedur yang ditentukan.	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11. Evaluasi Berkala	Sistem komputeri sasi harus dievaluasi secara berkala untuk memastikan bahwa mereka tetap dalam keadaan valid dan sesuai dengan GMP. Evaluasi tersebut harus mencakup, jika sesuai, rentang fungsionalitas saat ini, catatan penyimpangan, insiden, masalah, riwayat peningkatan, kinerja, keandalan , keamanan, dan laporan status validasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.1. Keamanan - Orang yang Berwenang	Kontrol fisik dan/atau logis harus dilakukan untuk membatasi akses ke sistem komputerisasi kepada orang yang berwenang. Metode yang sesuai untuk mencegah masuk secara tidak sah ke sistem dapat mencakup penggunaan kunci, kartu pass, kode pribadi dengan kata sandi, biometrik, akses terbatas ke peralatan komputer dan area penyimpanan data.	codebuild-project-environment-privileged-periksa	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan lingkungan CodeBuild proyek Amazon Anda tidak mengaktifkan mode istimewa. Pengaturan ini harus dinonaktifkan untuk mencegah akses yang tidak diinginkan ke Docker APIs serta perangkat keras yang mendasarinya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.1. Keamanan - Orang yang Berwenang	Kontrol fisik dan/atau logis harus dilakukan untuk membatasi akses ke sistem komputerisasi kepada orang yang berwenang. Metode yang sesuai untuk mencegah masuk secara tidak sah ke sistem dapat mencakup penggunaan kunci, kartu pass, kode pribadi dengan kata sandi, biometrik, akses terbatas ke peralatan komputer dan area penyimpanan data.	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.1. Keamanan - Orang yang Berwenang	Kontrol fisik dan/atau logis harus dilakukan untuk membatasi akses ke sistem komputerisasi kepada orang yang berwenang. Metode yang sesuai untuk mencegah masuk secara tidak sah ke sistem dapat mencakup penggunaan kunci, kartu pass, kode pribadi dengan kata sandi, biometrik, akses terbatas ke peralatan komputer dan area penyimpanan data.	ecs-containers-nonprivileged	Untuk membantu menerapkan prinsip hak istimewa paling rendah, definisi tugas Amazon Elastic Container Service (Amazon ECS) seharusnya tidak mengaktifkan hak istimewa yang ditinggikan. Ketika parameter ini benar, wadah diberikan hak istimewa yang ditinggikan pada instance wadah host (mirip dengan pengguna root).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.1. Keamanan - Orang yang Berwenang	Kontrol fisik dan/atau logis harus dilakukan untuk membatasi akses ke sistem komputerisasi kepada orang yang berwenang. Metode yang sesuai untuk mencegah masuk secara tidak sah ke sistem dapat mencakup penggunaan kunci, kartu pass, kode pribadi dengan kata sandi, biometrik, akses terbatas ke peralatan komputer dan area penyimpanan data.	ecs-containers-readonly-access	Mengaktifkan akses baca saja ke wadah Amazon Elastic Container Service (ECS) dapat membantu mematuhi prinsip hak istimewa yang paling rendah. Opsi ini dapat mengurangi vektor serangan karena sistem file instance container tidak dapat dimodifikasi kecuali jika memiliki izin baca-tulis eksplisit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.1. Keamanan - Orang yang Berwenang	Kontrol fisik dan/atau logis harus dilakukan untuk membatasi akses ke sistem komputeri sasi kepada orang yang berwenang. Metode yang sesuai untuk mencegah masuk secara tidak sah ke sistem dapat mencakup penggunaa n kunci, kartu pass, kode pribadi dengan kata sandi, biometrik , akses terbatas ke peralatan komputer dan area penyimpan an data.	ecs-task-definition-nonroot-pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan bahwa pengguna non-root ditunjuk untuk mengakses definisi tugas Amazon Elastic Container Service (Amazon ECS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.1. Keamanan - Orang yang Berwenang	Kontrol fisik dan/atau logis harus dilakukan untuk membatasi akses ke sistem komputeri sasi kepada orang yang berwenang. Metode yang sesuai untuk mencegah masuk secara tidak sah ke sistem dapat mencakup penggunaa n kunci, kartu pass, kode pribadi dengan kata sandi, biometrik , akses terbatas ke peralatan komputer dan area penyimpan an data.	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.1. Keamanan - Orang yang Berwenang	Kontrol fisik dan/atau logis harus dilakukan untuk membatasi akses ke sistem komputerisasi kepada orang yang berwenang. Metode yang sesuai untuk mencegah masuk secara tidak sah ke sistem dapat mencakup penggunaan kunci, kartu pass, kode pribadi dengan kata sandi, biometrik, akses terbatas ke peralatan komputer dan area penyimpanan data.	efs-access-point-enforce-root-direktori	Menegakkan direktori root untuk jalur akses Amazon Elastic File System (Amazon EFS) membantu membatasi akses data dengan memastikan bahwa pengguna jalur akses hanya dapat menjangkau file dari subdirektori yang ditentukan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.1. Keamanan - Orang yang Berwenang	Kontrol fisik dan/atau logis harus dilakukan untuk membatasi akses ke sistem komputeri sasi kepada orang yang berwenang. Metode yang sesuai untuk mencegah masuk secara tidak sah ke sistem dapat mencakup penggunaa n kunci, kartu pass, kode pribadi dengan kata sandi, biometrik , akses terbatas ke peralatan komputer dan area penyimpan an data.	efs-access-point-enforce-identitas pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan penegakan pengguna diaktifkan untuk Amazon Elastic File System (Amazon EFS) Anda. Saat diaktifkan, Amazon EFS mengganti kan pengguna dan grup klien NFS IDs dengan identitas yang dikonfigurasi pada titik akses untuk semua operasi sistem file dan hanya memberika n akses ke identitas pengguna yang diberlakukan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.1. Keamanan - Orang yang Berwenang	Kontrol fisik dan/atau logis harus dilakukan untuk membatasi akses ke sistem komputerisasi kepada orang yang berwenang. Metode yang sesuai untuk mencegah masuk secara tidak sah ke sistem dapat mencakup penggunaan kunci, kartu pass, kode pribadi dengan kata sandi, biometrik, akses terbatas ke peralatan komputer dan area penyimpanan data.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.1. Keamanan - Orang yang Berwenang	Kontrol fisik dan/atau logis harus dilakukan untuk membatasi akses ke sistem komputerisasi kepada orang yang berwenang. Metode yang sesuai untuk mencegah masuk secara tidak sah ke sistem dapat mencakup penggunaan kunci, kartu pass, kode pribadi dengan kata sandi, biometrik, akses terbatas ke peralatan komputer dan area penyimpanan data.	opensearch-access-control-enabled	Pastikan kontrol akses berbutir halus diaktifkan di domain Layanan Amazon OpenSearch Anda. Kontrol akses berbutir halus menyediakan mekanisme otorisasi yang disempurnakan untuk mencapai akses yang paling tidak memiliki hak istimewa ke domain Layanan Amazon. OpenSearch Ini memungkinkan kontrol akses berbasis peran ke domain, serta indeks, dokumen, dan keamanan tingkat lapangan, dukungan untuk dasbor OpenSearch Layanan multi-tenancy, dan otentikasi dasar HTTP untuk Layanan dan Kibana. OpenSearch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.1. Keamanan - Orang yang Berwenang	Kontrol fisik dan/atau logis harus dilakukan untuk membatasi akses ke sistem komputerisasi kepada orang yang berwenang. Metode yang sesuai untuk mencegah masuk secara tidak sah ke sistem dapat mencakup penggunaan kunci, kartu pass, kode pribadi dengan kata sandi, biometrik, akses terbatas ke peralatan komputer dan area penyimpanan data.	rds-instance-iam-authentication-diaktifkan	Pastikan autentikasi AWS Identity and Access Management (IAM) diaktifkan pada instans Amazon Relational Database Service (Amazon RDS) untuk mengontrol akses ke sistem dan aset. Ini memberlakukan lalu lintas jaringan ke dan dari database yang akan dienkripsi menggunakan Secure Sockets Layer (SSL). Anda tidak diharuskan untuk menyimpan kredensi pengguna dalam database, karena otentikasi dikelola secara eksternal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.1. Keamanan - Orang yang Berwenang	Kontrol fisik dan/atau logis harus dilakukan untuk membatasi akses ke sistem komputerisasi kepada orang yang berwenang. Metode yang sesuai untuk mencegah masuk secara tidak sah ke sistem dapat mencakup penggunaan kunci, kartu pass, kode pribadi dengan kata sandi, biometrik, akses terbatas ke peralatan komputer dan area penyimpanan data.	s3- bucket-acl-prohibited	Aturan ini memeriksa untuk melihat apakah Daftar Kontrol Akses (ACLs) digunakan untuk kontrol akses di Bucket Amazon S3. ACLs adalah mekanisme kontrol akses lama untuk bucket Amazon S3 yang AWS mendahului Identity and Access Management (IAM). Sebagai gantinya ACLs, ini adalah praktik terbaik untuk menggunakan kebijakan IAM atau kebijakan bucket S3 untuk mengelola akses ke bucket S3 Anda dengan lebih mudah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.1. Keamanan - Orang yang Berwenang	Kontrol fisik dan/atau logis harus dilakukan untuk membatasi akses ke sistem komputerisasi kepada orang yang berwenang. Metode yang sesuai untuk mencegah masuk secara tidak sah ke sistem dapat mencakup penggunaan kunci, kartu pass, kode pribadi dengan kata sandi, biometrik, akses terbatas ke peralatan komputer dan area penyimpanan data.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.1. Keamanan - Orang yang Berwenang	Kontrol fisik dan/atau logis harus dilakukan untuk membatasi akses ke sistem komputeri sasi kepada orang yang berwenang. Metode yang sesuai untuk mencegah masuk secara tidak sah ke sistem dapat mencakup penggunaa n kunci, kartu pass, kode pribadi dengan kata sandi, biometrik , akses terbatas ke peralatan komputer dan area penyimpan an data.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.1. Keamanan - Orang yang Berwenang	Kontrol fisik dan/atau logis harus dilakukan untuk membatasi akses ke sistem komputerisasi kepada orang yang berwenang. Metode yang sesuai untuk mencegah masuk secara tidak sah ke sistem dapat mencakup penggunaan kunci, kartu pass, kode pribadi dengan kata sandi, biometrik, akses terbatas ke peralatan komputer dan area penyimpanan data.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.1. Keamanan - Orang yang Berwenang	Kontrol fisik dan/atau logis harus dilakukan untuk membatasi akses ke sistem komputerisasi kepada orang yang berwenang. Metode yang sesuai untuk mencegah masuk secara tidak sah ke sistem dapat mencakup penggunaan kunci, kartu pass, kode pribadi dengan kata sandi, biometrik, akses terbatas ke peralatan komputer dan area penyimpanan data.	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi, pengembalian, dan pendelegasian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
12.1. Keamanan - Orang yang Berwenang	Kontrol fisik dan/atau logis harus dilakukan untuk membatasi akses ke sistem komputerisasi kepada orang yang berwenang. Metode yang sesuai untuk mencegah masuk secara tidak sah ke sistem dapat mencakup penggunaan kunci, kartu pass, kode pribadi dengan kata sandi, biometrik, akses terbatas ke peralatan komputer dan area penyimpanan data.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.1. Keamanan - Orang yang Berwenang	Kontrol fisik dan/atau logis harus dilakukan untuk membatasi akses ke sistem komputeri sasi kepada orang yang berwenang. Metode yang sesuai untuk mencegah masuk secara tidak sah ke sistem dapat mencakup penggunaa n kunci, kartu pass, kode pribadi dengan kata sandi, biometrik , akses terbatas ke peralatan komputer dan area penyimpan an data.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.1. Keamanan - Orang yang Berwenang	Kontrol fisik dan/atau logis harus dilakukan untuk membatasi akses ke sistem komputeri sasi kepada orang yang berwenang. Metode yang sesuai untuk mencegah masuk secara tidak sah ke sistem dapat mencakup penggunaa n kunci, kartu pass, kode pribadi dengan kata sandi, biometrik , akses terbatas ke peralatan komputer dan area penyimpan an data.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.1. Keamanan - Orang yang Berwenang	Kontrol fisik dan/atau logis harus dilakukan untuk membatasi akses ke sistem komputerisasi kepada orang yang berwenang. Metode yang sesuai untuk mencegah masuk secara tidak sah ke sistem dapat mencakup penggunaan kunci, kartu pass, kode pribadi dengan kata sandi, biometrik, akses terbatas ke peralatan komputer dan area penyimpanan data.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.1. Keamanan - Orang yang Berwenang	Kontrol fisik dan/atau logis harus dilakukan untuk membatasi akses ke sistem komputeri sasi kepada orang yang berwenang. Metode yang sesuai untuk mencegah masuk secara tidak sah ke sistem dapat mencakup penggunaa n kunci, kartu pass, kode pribadi dengan kata sandi, biometrik , akses terbatas ke peralatan komputer dan area penyimpan an data.	sagemaker-notebook -no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.3. Keamanan - Jejak Audit Otorisasi	Pembuatan, perubahan, dan pembatalan otorisasi akses harus dicatat.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
12.4. Keamanan - Jejak Audit	Sistem manajemen untuk data dan dokumen harus dirancang untuk mencatat identitas operator yang memasuki, mengubah, mengonfirmasi atau menghapus data termasuk tanggal dan waktu.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.4. Keamanan - Jejak Audit	Sistem manajemen untuk data dan dokumen harus dirancang untuk mencatat identitas operator yang memasuki, mengubah, mengonfirmasi atau menghapus data termasuk tanggal dan waktu.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
12.4. Keamanan - Jejak Audit	Sistem manajemen untuk data dan dokumen harus dirancang untuk mencatat identitas operator yang memasuki, mengubah, mengonfirmasi atau menghapus data termasuk tanggal dan waktu.	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.4. Keamanan - Jejak Audit	Sistem manajemen untuk data dan dokumen harus dirancang untuk mencatat identitas operator yang memasuki, mengubah, mengonfirmasi atau menghapus data termasuk tanggal dan waktu.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.4. Keamanan - Jejak Audit	Sistem manajemen untuk data dan dokumen harus dirancang untuk mencatat identitas operator yang memasuki, mengubah, mengonfirmasi atau menghapus data termasuk tanggal dan waktu.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.4. Keamanan - Jejak Audit	Sistem manajemen untuk data dan dokumen harus dirancang untuk mencatat identitas operator yang memasuki, mengubah, mengonfirmasi atau menghapus data termasuk tanggal dan waktu.	opensearch-audit-logging-enabled	Pastikan pencatatan audit diaktifkan di domain OpenSearch Layanan Amazon Anda. Pencatatan audit memungkinkan Anda melacak aktivitas pengguna di OpenSearch domain Anda, termasuk keberhasilan dan kegagalan otentikasi, permintaan, perubahan indeks OpenSearch, dan kueri penelusuran yang masuk.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.4. Keamanan - Jejak Audit	Sistem manajemen untuk data dan dokumen harus dirancang untuk mencatat identitas operator yang memasuki, mengubah, mengonfirmasi atau menghapus data termasuk tanggal dan waktu.	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
12.4. Keamanan - Jejak Audit	Sistem manajemen untuk data dan dokumen harus dirancang untuk mencatat identitas operator yang memasuki, mengubah, mengonfirmasi atau menghapus data termasuk tanggal dan waktu.	redshift-audit-logging-enabled	Untuk menangkap informasi tentang koneksi dan aktivitas pengguna di klaster Amazon Redshift, pastikan pencatatan audit diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.4. Keamanan - Jejak Audit	Sistem manajemen untuk data dan dokumen harus dirancang untuk mencatat identitas operator yang memasuki, mengubah, mengonfirmasi atau menghapus data termasuk tanggal dan waktu.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
12.4. Keamanan - Jejak Audit	Sistem manajemen untuk data dan dokumen harus dirancang untuk mencatat identitas operator yang memasuki, mengubah, mengonfirmasi atau menghapus data termasuk tanggal dan waktu.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.4. Keamanan - Jejak Audit	Sistem manajemen untuk data dan dokumen harus dirancang untuk mencatat identitas operator yang memasuki, mengubah, mengonfirmasi atau menghapus data termasuk tanggal dan waktu.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.4. Keamanan - Jejak Audit	Sistem manajemen untuk data dan dokumen harus dirancang untuk mencatat identitas operator yang memasuki, mengubah, mengonfirmasi atau menghapus data termasuk tanggal dan waktu.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
13. Manajemen Insiden	Semua insiden, tidak hanya kegagalan sistem dan kesalahan data, harus dilaporkan dan dinilai. Akar penyebab insiden kritis harus diidentifikasi dan harus menjadi dasar tindakan korektif dan pencegahan.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
13. Manajemen Insiden	Semua insiden, tidak hanya kegagalan sistem dan kesalahan data, harus dilaporkan dan dinilai. Akar penyebab insiden kritis harus diidentifikasi dan harus menjadi dasar tindakan korektif dan pencegahan.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengaturan alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengaturan alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengatura n alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengaturan alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengaturan alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengatura n alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengaturan alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengaturan alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengatura n alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengaturan alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengaturan alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	ebs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengaturan alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengatura n alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	efs-in-backup-plan	Untuk membantu proses pencadang an data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengaturan alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	efs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengatura n alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengatura n alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	elbv2-multiple-az	Elastic Load Balancing (ELB) secara otomatis mendistribusikan lalu lintas masuk Anda di beberapa target, seperti EC2 instans, kontainer, dan alamat IP, di zona ketersedi aan. Untuk memastika n ketersediaan tinggi, pastikan ELB Anda telah mendaftarkan instans dari beberapa Availability Zone.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengaturan alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengaturan alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengatura n alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	lambda-vpc-multi-az-periksa	Jika fungsi AWS Lambda Anda dikonfigurasi untuk terhubung ke virtual private cloud (VPC) di akun Anda, gunakan fungsi AWS Lambda di setidaknya dua Availability Zone yang berbeda untuk memastikan bahwa fungsi Anda tersedia untuk memproses peristiwa jika terjadi gangguan layanan di satu zona.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengatura n alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	opensearch-data-no de-fault-toleransi	Amazon OpenSearch Service (OpenSearch Service) memerlukan setidaknya tiga node data untuk ketersedi aan tinggi dan toleransi kesalahan. Menyebarkan domain OpenSearch Layanan dengan setidakny a tiga node data memastikan operasi klaster jika node gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengaturan alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	rds-cluster-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengaturan alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengatura n alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengatura n alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	redshift-backup-en abled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifka n untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengatura n alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengatura n alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengaturan alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengaturan alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	rds-cluster-multi-az-diaktifkan	Cluster Amazon Relational Database Service (Amazon RDS) harus mengaktifkan replikasi Multi-AZ untuk membantu ketersediaan data yang disimpan. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengaturan alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
16. Kesinambungan Bisnis	Untuk ketersediaan sistem komputerisasi yang mendukung proses kritis, ketentuan harus dibuat untuk memastikan kesinambungan dukungan untuk proses tersebut jika terjadi kerusakan sistem (misalnya sistem manual atau alternatif). Waktu yang diperlukan untuk membawa pengatura n alternatif ke dalam penggunaan harus didasarkan pada risiko dan sesuai untuk sistem tertentu dan proses bisnis yang didukungnya. Pengaturan ini harus didokumentasikan dan diuji secara memadai.	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimpleme ntasikan untuk mencapai persyarat an ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivi tas jika salah satu koneksi Site-to-S ite VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivi tas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
17. Pengarsipan	Data dapat diarsipkan. Data ini harus diperiksa untuk aksesibilitas, keterbacaan, dan integritas. Jika perubahan yang relevan harus dilakukan pada sistem (misalnya peralatan komputer atau program), maka kemampuan untuk mengambil data harus dipastikan dan diuji.	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
17. Pengarsipan	Data dapat diarsipkan. Data ini harus diperiksa untuk aksesibilitas, keterbacaan, dan integritas. Jika perubahan yang relevan harus dilakukan pada sistem (misalnya peralatan komputer atau program), maka kemampuan untuk mengambil data harus dipastikan dan diuji.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
17. Pengarsipan	Data dapat diarsipkan. Data ini harus diperiksa untuk aksesibilitas, keterbacaan, dan integritas. Jika perubahan yang relevan harus dilakukan pada sistem (misalnya peralatan komputer atau program), maka kemampuan untuk mengambil data harus dipastikan dan diuji.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
17. Pengarsipan	Data dapat diarsipkan. Data ini harus diperiksa untuk aksesibilitas, keterbacaan, dan integritas. Jika perubahan yang relevan harus dilakukan pada sistem (misalnya peralatan komputer atau program), maka kemampuan untuk mengambil data harus dipastikan dan diuji.	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
17. Pengarsipan	Data dapat diarsipkan. Data ini harus diperiksa untuk aksesibilitas, keterbacaan, dan integritas. Jika perubahan yang relevan harus dilakukan pada sistem (misalnya peralatan komputer atau program), maka kemampuan untuk mengambil data harus dipastikan dan diuji.	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
17. Pengarsipan	Data dapat diarsipkan. Data ini harus diperiksa untuk aksesibilitas, keterbacaan, dan integritas. Jika perubahan yang relevan harus dilakukan pada sistem (misalnya peralatan komputer atau program), maka kemampuan untuk mengambil data harus dipastikan dan diuji.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
17. Pengarsipan	Data dapat diarsipkan. Data ini harus diperiksa untuk aksesibilitas, keterbacaan, dan integritas. Jika perubahan yang relevan harus dilakukan pada sistem (misalnya peralatan komputer atau program), maka kemampuan untuk mengambil data harus dipastikan dan diuji.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
17. Pengarsipan	Data dapat diarsipkan. Data ini harus diperiksa untuk aksesibilitas, keterbacaan, dan integritas. Jika perubahan yang relevan harus dilakukan pada sistem (misalnya peralatan komputer atau program), maka kemampuan untuk mengambil data harus dipastikan dan diuji.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
17. Pengarsipan	Data dapat diarsipkan. Data ini harus diperiksa untuk aksesibilitas, keterbacaan, dan integritas. Jika perubahan yang relevan harus dilakukan pada sistem (misalnya peralatan komputer atau program), maka kemampuan untuk mengambil data harus dipastikan dan diuji.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
17. Pengarsipan	Data dapat diarsipkan. Data ini harus diperiksa untuk aksesibilitas, keterbacaan, dan integritas. Jika perubahan yang relevan harus dilakukan pada sistem (misalnya peralatan komputer atau program), maka kemampuan untuk mengambil data harus dipastikan dan diuji.	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
17. Pengarsipan	Data dapat diarsipkan. Data ini harus diperiksa untuk aksesibilitas, keterbacaan, dan integritas. Jika perubahan yang relevan harus dilakukan pada sistem (misalnya peralatan komputer atau program), maka kemampuan untuk mengambil data harus dipastikan dan diuji.	ebs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
17. Pengarsipan	Data dapat diarsipkan. Data ini harus diperiksa untuk aksesibilitas, keterbacaan, dan integritas. Jika perubahan yang relevan harus dilakukan pada sistem (misalnya peralatan komputer atau program), maka kemampuan untuk mengambil data harus dipastikan dan diuji.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
17. Pengarsipan	Data dapat diarsipkan. Data ini harus diperiksa untuk aksesibilitas, keterbacaan, dan integritas. Jika perubahan yang relevan harus dilakukan pada sistem (misalnya peralatan komputer atau program), maka kemampuan untuk mengambil data harus dipastikan dan diuji.	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
17. Pengarsipan	Data dapat diarsipkan. Data ini harus diperiksa untuk aksesibilitas, keterbacaan, dan integritas. Jika perubahan yang relevan harus dilakukan pada sistem (misalnya peralatan komputer atau program), maka kemampuan untuk mengambil data harus dipastikan dan diuji.	efs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
17. Pengarsipan	Data dapat diarsipkan. Data ini harus diperiksa untuk aksesibilitas, keterbacaan, dan integritas. Jika perubahan yang relevan harus dilakukan pada sistem (misalnya peralatan komputer atau program), maka kemampuan untuk mengambil data harus dipastikan dan diuji.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
17. Pengarsipan	Data dapat diarsipkan. Data ini harus diperiksa untuk aksesibilitas, keterbacaan, dan integritas. Jika perubahan yang relevan harus dilakukan pada sistem (misalnya peralatan komputer atau program), maka kemampuan untuk mengambil data harus dipastikan dan diuji.	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
17. Pengarsipan	Data dapat diarsipkan. Data ini harus diperiksa untuk aksesibilitas, keterbacaan, dan integritas. Jika perubahan yang relevan harus dilakukan pada sistem (misalnya peralatan komputer atau program), maka kemampuan untuk mengambil data harus dipastikan dan diuji.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relational Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
17. Pengarsipan	Data dapat diarsipkan. Data ini harus diperiksa untuk aksesibilitas, keterbacaan, dan integritas. Jika perubahan yang relevan harus dilakukan pada sistem (misalnya peralatan komputer atau program), maka kemampuan untuk mengambil data harus dipastikan dan diuji.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
17. Pengarsipan	Data dapat diarsipkan. Data ini harus diperiksa untuk aksesibilitas, keterbacaan, dan integritas. Jika perubahan yang relevan harus dilakukan pada sistem (misalnya peralatan komputer atau program), maka kemampuan untuk mengambil data harus dipastikan dan diuji.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
17. Pengarsipan	Data dapat diarsipkan. Data ini harus diperiksa untuk aksesibilitas, keterbacaan, dan integritas. Jika perubahan yang relevan harus dilakukan pada sistem (misalnya peralatan komputer atau program), maka kemampuan untuk mengambil data harus dipastikan dan diuji.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk GxP EU Annex 11.

Praktik Terbaik Operasional untuk Keamanan HIPAA

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk

membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA) dan aturan Config yang dikelola. AWS Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan berhubungan dengan satu atau beberapa kontrol HIPAA. Kontrol HIPAA dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

Paket Kesesuaian ini divalidasi oleh AWS Security Assurance Services LLC (AWS SAS), yang merupakan tim dari Payment Card Industry Qualified Security Assesors (QSAs), HITRUST Certified Common Security Framework Practitioners (CCSFPs), dan profesional kepatuhan yang disertifikasi untuk memberikan panduan dan penilaian untuk berbagai kerangka kerja industri. AWS Profesional SAS merancang Paket Kesesuaian ini untuk memungkinkan pelanggan menyelaraskan dengan subset HIPAA.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (A)	(A) Analisis risiko (Wajib). Melakukan penilaian yang akurat dan menyeluruh terhadap potensi risiko dan kerentana n terhadap kerahasia an, integritas, dan ketersediaan informasi kesehatan yang dilindungi secara elektronik yang dimiliki oleh entitas yang tercakup.	annual-risk-assess ment-performed (Pemeriksaan Proses)	Lakukan penilaian risiko tahunan pada organisasi Anda. Penilaian risiko dapat membantu dalam menentuka n kemungkinan dan dampak dari risiko dan/atau kerentana n yang diidentifikasi yang mempengaruhi suatu organisasi.
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).		Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild . Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredenal masuk dalam lingkungan proyek Codebuild . AWS Gunakan OAuth alih-alih token akses pribadi atau kredensyal masuk untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan cadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	elasticsearch-encr ypted-at-rest	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk domain OpenSearc h Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) menyediakan ketersediaan dan daya tahan yang ditingkatkan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			segera setelah failover selesai.
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (1) (ii) (B)	(B) Manajemen risiko (Wajib). Menerapkan langkah-langkah keamanan yang cukup untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi Pasal 164.306 (a).	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktifkan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediakan sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi, pengembalian, dan pendelegasian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensi yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	ecs-containers-readonly-access	Mengaktifkan akses baca saja ke wadah Amazon Elastic Container Service (ECS) dapat membantu mematuhi prinsip hak istimewa yang paling rendah. Opsi ini dapat mengurangi vektor serangan karena sistem file instance container tidak dapat dimodifikasi kecuali jika memiliki izin baca-tulis eksplisit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	s3- bucket-acl-prohibited	Aturan ini memeriksa untuk melihat apakah Daftar Kontrol Akses (ACLs) digunakan untuk kontrol akses di Bucket Amazon S3. ACLs adalah mekanisme kontrol akses lama untuk bucket Amazon S3 yang AWS mendahului Identity and Access Management (IAM). Sebagai gantinya ACLs, ini adalah praktik terbaik untuk menggunakan kebijakan IAM atau kebijakan bucket S3 untuk mengelola akses ke bucket S3 Anda dengan lebih mudah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild. Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredenal masuk dalam lingkungan proyek Codebuild. AWS Gunakan OAuth alih-alih token akses pribadi atau kredensyal masuk untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (i)	(3) (i) Standar: Keamanan tenaga kerja. Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat ke informasi kesehatan yang dilindungi secara elektronik, sebagaimana diatur dalam paragraf (a) (4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan ayat (a) (4) bagian ini memperoleh akses ke informasi kesehatan yang dilindungi secara elektronik.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (ii) (A)	(A) and/or supervisi on (Addressable). Implement procedure s for the authorization and/or Pengawasa n otorisasi anggota tenaga kerja yang bekerja dengan informasi kesehatan yang dilindungi secara elektronik atau di lokasi di mana informasi tersebut dapat diakses.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (ii) (A)	(A) and/or supervisi on (Addressable). Implement procedure s for the authorization and/or Pengawasa n otorisasi anggota tenaga kerja yang bekerja dengan informasi kesehatan yang dilindungi secara elektronik atau di lokasi yang dapat diakses.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (ii) (A)	(A) and/or supervisi on (Addressable). Implement procedure s for the authorization and/or Pengawasa n otorisasi anggota tenaga kerja yang bekerja dengan informasi kesehatan yang dilindungi secara elektronik atau di lokasi yang dapat diakses.	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
164.308 (a) (3) (ii) (A)	(A) and/or supervisi on (Addressable). Implement procedure s for the authorization and/or Pengawasa n otorisasi anggota tenaga kerja yang bekerja dengan informasi kesehatan yang dilindungi secara elektronik atau di lokasi yang dapat diakses.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (ii) (A)	(A) and/or supervisi on (Addressable). Implement procedure s for the authorization and/or Pengawasa n otorisasi anggota tenaga kerja yang bekerja dengan informasi kesehatan yang dilindungi secara elektronik atau di lokasi yang dapat diakses.	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (ii) (A)	(A) and/or supervisi on (Addressable). Implement procedure s for the authorization and/or Pengawasa n otorisasi anggota tenaga kerja yang bekerja dengan informasi kesehatan yang dilindungi secara elektronik atau di lokasi yang dapat diakses.	iam-user-no-policies-periksa	Aturan ini memastika n kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapka n hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.
164.308 (a) (3) (ii) (A)	(A) and/or supervisi on (Addressable). Implement procedure s for the authorization and/or Pengawasa n otorisasi anggota tenaga kerja yang bekerja dengan informasi kesehatan yang dilindungi secara elektronik atau di lokasi yang dapat diakses.	iam-policy-no-stat ements-with-full-a ccess	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (ii) (A)	(A) and/or supervisi on (Addressable). Implement procedure s for the authorization and/or Pengawasa n otorisasi anggota tenaga kerja yang bekerja dengan informasi kesehatan yang dilindungi secara elektronik atau di lokasi yang dapat diakses.	ec2- instance-profile-a ttached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirk an profil instans ke instans Anda dapat membantu pengelola an hak istimewa dan izin paling sedikit.
164.308 (a) (3) (ii) (A)	(A) and/or supervisi on (Addressable). Implement procedure s for the authorization and/or Pengawasa n otorisasi anggota tenaga kerja yang bekerja dengan informasi kesehatan yang dilindungi secara elektronik atau di lokasi yang dapat diakses.	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (ii) (A)	(A) and/or supervisi on (Addressable). Implement procedure s for the authorization and/or Pengawasa n otorisasi anggota tenaga kerja yang bekerja dengan informasi kesehatan yang dilindungi secara elektronik atau di lokasi yang dapat diakses.	ecs-containers-rea donly-access	Mengaktifkan akses baca saja ke wadah Amazon Elastic Container Service (ECS) dapat membantu mematuhi prinsip hak istimewa yang paling rendah. Opsi ini dapat mengurangi vektor serangan karena sistem file instance container tidak dapat dimodifikasi kecuali jika memiliki izin baca-tulis eksplisit.
164.308 (a) (3) (ii) (A)	(A) and/or supervisi on (Addressable). Implement procedure s for the authorization and/or Pengawasa n otorisasi anggota tenaga kerja yang bekerja dengan informasi kesehatan yang dilindungi secara elektronik atau di lokasi yang dapat diakses.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (ii) (A)	(A) and/or supervision (Addressable). Implement procedures for the authorization and/or Pengawasan otorisasi anggota tenaga kerja yang bekerja dengan informasi kesehatan yang dilindungi secara elektronik atau di lokasi yang dapat diakses.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
164.308 (a) (3) (ii) (A)	(A) and/or supervision (Addressable). Implement procedures for the authorization and/or Pengawasan otorisasi anggota tenaga kerja yang bekerja dengan informasi kesehatan yang dilindungi secara elektronik atau di lokasi yang dapat diakses.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (ii) (A)	(A) and/or supervisi on (Addressable). Implement procedure s for the authorization and/or Pengawasa n otorisasi anggota tenaga kerja yang bekerja dengan informasi kesehatan yang dilindungi secara elektronik atau di lokasi yang dapat diakses.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (ii) (A)	(A) and/or supervisi on (Addressable). Implement procedure s for the authorization and/or Pengawasa n otorisasi anggota tenaga kerja yang bekerja dengan informasi kesehatan yang dilindungi secara elektronik atau di lokasi yang dapat diakses.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (ii) (A)	(A) and/or supervisi on (Addressable). Implement procedure s for the authorization and/or Pengawasa n otorisasi anggota tenaga kerja yang bekerja dengan informasi kesehatan yang dilindungi secara elektronik atau di lokasi yang dapat diakses.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediak an metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinc i untuk permintaa n yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (ii) (A)	(A) and/or supervisi on (Addressable). Implement procedure s for the authorization and/or Pengawasa n otorisasi anggota tenaga kerja yang bekerja dengan informasi kesehatan yang dilindungi secara elektronik atau di lokasi yang dapat diakses.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
164.308 (a) (3) (ii) (A)	(A) and/or supervisi on (Addressable). Implement procedure s for the authorization and/or Pengawasa n otorisasi anggota tenaga kerja yang bekerja dengan informasi kesehatan yang dilindungi secara elektronik atau di lokasi yang dapat diakses.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (ii) (A)	(A) and/or supervision (Addressable). Implement procedures for the authorization and/or Pengawasan otorisasi anggota tenaga kerja yang bekerja dengan informasi kesehatan yang dilindungi secara elektronik atau di lokasi yang dapat diakses.	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (ii) (B)	(B) Prosedur pembersihan tenaga kerja (Dapat dialamatkan). Menerapkan prosedur untuk menentukan bahwa akses anggota tenaga kerja ke informasi kesehatan yang dilindungi secara elektronik adalah tepat.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (ii) (B)	(B) Prosedur pembersihan tenaga kerja (Dapat dialamatkan). Menerapkan prosedur untuk menentukan bahwa akses anggota tenaga kerja ke informasi kesehatan yang dilindungi secara elektronik adalah tepat.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (ii) (B)	(B) Prosedur pembersihan tenaga kerja (Dapat dialamatkan). Menerapkan prosedur untuk menentukan bahwa akses anggota tenaga kerja ke informasi kesehatan yang dilindungi secara elektronik adalah tepat.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (ii) (B)	(B) Prosedur pembersihan tenaga kerja (Dapat dialamatkan). Menerapkan prosedur untuk menentukan bahwa akses anggota tenaga kerja ke informasi kesehatan yang dilindungi secara elektronik adalah tepat.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.
164.308 (a) (3) (ii) (B)	(B) Prosedur pembersihan tenaga kerja (Dapat dialamatkan). Menerapkan prosedur untuk menentukan bahwa akses anggota tenaga kerja ke informasi kesehatan yang dilindungi secara elektronik adalah tepat.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (ii) (B)	(B) Prosedur pembersihan tenaga kerja (Dapat dialamatkan). Menerapkan prosedur untuk menentukan bahwa akses anggota tenaga kerja ke informasi kesehatan yang dilindungi secara elektronik adalah tepat.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (ii) (B)	(B) Prosedur pembersihan tenaga kerja (Dapat dialamatkan). Menerapkan prosedur untuk menentukan bahwa akses anggota tenaga kerja ke informasi kesehatan yang dilindungi secara elektronik adalah tepat.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.
164.308 (a) (3) (ii) (B)	(B) Prosedur pembersihan tenaga kerja (Dapat dialamatkan). Menerapkan prosedur untuk menentukan bahwa akses anggota tenaga kerja ke informasi kesehatan yang dilindungi secara elektronik adalah tepat.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (ii) (B)	(B) Prosedur pembersihan tenaga kerja (Dapat dialamatkan). Menerapkan prosedur untuk menentukan bahwa akses anggota tenaga kerja ke informasi kesehatan yang dilindungi secara elektronik adalah tepat.	ecs-containers-readonly-access	Mengaktifkan akses baca saja ke wadah Amazon Elastic Container Service (ECS) dapat membantu mematuhi prinsip hak istimewa yang paling rendah. Opsi ini dapat mengurangi vektor serangan karena sistem file instance container tidak dapat dimodifikasi kecuali jika memiliki izin baca-tulis eksplisit.
164.308 (a) (3) (ii) (B)	(B) Prosedur pembersihan tenaga kerja (Dapat dialamatkan). Menerapkan prosedur untuk menentukan bahwa akses anggota tenaga kerja ke informasi kesehatan yang dilindungi secara elektronik adalah tepat.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (ii) (B)	(B) Prosedur pembersihan tenaga kerja (Dapat dialamatkan). Menerapkan prosedur untuk menentukan bahwa akses anggota tenaga kerja ke informasi kesehatan yang dilindungi secara elektronik adalah tepat.	s3- bucket-acl-prohibited	Aturan ini memeriksa untuk melihat apakah Daftar Kontrol Akses (ACLs) digunakan untuk kontrol akses di Bucket Amazon S3. ACLs adalah mekanisme kontrol akses lama untuk bucket Amazon S3 yang AWS mendahului Identity and Access Management (IAM). Sebagai gantinya ACLs, ini adalah praktik terbaik untuk menggunakan kebijakan IAM atau kebijakan bucket S3 untuk mengelola akses ke bucket S3 Anda dengan lebih mudah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (3) (ii) (C)	(C) Prosedur penghentian (Dapat dialamatkan). Menerapkan prosedur untuk menghenti kan akses ke informasi kesehatan yang dilindungi secara elektronik ketika pekerjaan anggota angkatan kerja berakhir atau sebagaimana disyaratkan oleh penentuan yang dibuat sebagaima na ditentukan dalam paragraf (a) (3) (ii) (B) bagian ini.	access-keys-rotated	Kredensi diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastika n kunci akses IAM diputar sebagaima na ditentukan oleh kebijakan organisas i. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurang i dampak bisnis jika kunci dikompromikan. Aturan ini memerluka n nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (i)	(4) (i) Standar: Manajemen akses informasi. Menerapkan kebijakan dan prosedur untuk mengizinkan akses ke informasi kesehatan yang dilindungi secara elektronik yang konsisten dengan persyaratan yang berlaku dari subbagian E bagian ini.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktifkan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediakan sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (i)	(4) (i) Standar: Manajemen akses informasi. Menerapkan kebijakan dan prosedur untuk mengizinkan akses ke informasi kesehatan yang dilindungi secara elektronik yang konsisten dengan persyaratan yang berlaku dari subbagian E bagian ini.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (i)	(4) (i) Standar: Manajemen akses informasi. Menerapkan kebijakan dan prosedur untuk mengizinkan akses ke informasi kesehatan yang dilindungi secara elektronik yang konsisten dengan persyaratan yang berlaku dari subbagian E bagian ini.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (i)	(4) (i) Standar: Manajemen akses informasi. Menerapkan kebijakan dan prosedur untuk mengizinkan akses ke informasi kesehatan yang dilindungi secara elektronik yang konsisten dengan persyaratan yang berlaku dari subbagian E bagian ini.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.
164.308 (a) (4) (i)	(4) (i) Standar: Manajemen akses informasi. Menerapkan kebijakan dan prosedur untuk mengizinkan akses ke informasi kesehatan yang dilindungi secara elektronik yang konsisten dengan persyaratan yang berlaku dari subbagian E bagian ini.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (i)	(4) (i) Standar: Manajemen akses informasi. Menerapkan kebijakan dan prosedur untuk mengizinkan akses ke informasi kesehatan yang dilindungi secara elektronik yang konsisten dengan persyaratan yang berlaku dari subbagian E bagian ini.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (i)	(4) (i) Standar: Manajemen akses informasi. Menerapkan kebijakan dan prosedur untuk mengizinkan akses ke informasi kesehatan yang dilindungi secara elektronik yang konsisten dengan persyaratan yang berlaku dari subbagian E bagian ini.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.
164.308 (a) (4) (i)	(4) (i) Standar: Manajemen akses informasi. Menerapkan kebijakan dan prosedur untuk mengizinkan akses ke informasi kesehatan yang dilindungi secara elektronik yang konsisten dengan persyaratan yang berlaku dari subbagian E bagian ini.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (i)	(4) (i) Standar: Manajemen akses informasi. Menerapkan kebijakan dan prosedur untuk mengizinkan akses ke informasi kesehatan yang dilindungi secara elektronik yang konsisten dengan persyaratan yang berlaku dari subbagian E bagian ini.	ecs-containers-readonly-access	Mengaktifkan akses baca saja ke wadah Amazon Elastic Container Service (ECS) dapat membantu mematuhi prinsip hak istimewa yang paling rendah. Opsi ini dapat mengurangi vektor serangan karena sistem file instance container tidak dapat dimodifikasi kecuali jika memiliki izin baca-tulis eksplisit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (i)	(4) (i) Standar: Manajemen akses informasi. Menerapkan kebijakan dan prosedur untuk mengizinkan akses ke informasi kesehatan yang dilindungi secara elektronik yang konsisten dengan persyaratan yang berlaku dari subbagian E bagian ini.	s3- bucket-acl-prohibited	Aturan ini memeriksa untuk melihat apakah Daftar Kontrol Akses (ACLs) digunakan untuk kontrol akses di Bucket Amazon S3. ACLs adalah mekanisme kontrol akses lama untuk bucket Amazon S3 yang AWS mendahului Identity and Access Management (IAM). Sebagai gantinya ACLs, ini adalah praktik terbaik untuk menggunakan kebijakan IAM atau kebijakan bucket S3 untuk mengelola akses ke bucket S3 Anda dengan lebih mudah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifka n untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	iam-user-no-policies-periksa	Aturan ini memastika n kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapka n hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	iam-user-unused-cr edentials-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensi yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCreden tialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	iam-policy-no-stat ements-with-full-a ccess	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	ec2- instance-profile-a ttached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirk an profil instans ke instans Anda dapat membantu pengelola an hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSear ch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerluka n gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	internet-gateway-a uthorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirk an ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	lambda-function-pu blic-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotens i menyebabkan degradasi ketersedi aan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	s3- account-level-publ ic-access -blok-per iodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	sagemaker-notebook -no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurk an ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCES S_KEY_ID dan AWS_SECRE T_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild . Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabk an paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredenal masuk dalam lingkungan proyek Codebuild . AWS Gunakan OAuth alih-alih token akses pribadi atau kredensyal masuk untuk memberika n otorisasi untuk mengakses GitHub atau repositori Bitbucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	autoscaling-launch -config-public-ip- dinonaktifkan	Jika Anda mengonfig urasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearinghouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapkan kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektronik dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	ecs-containers-readonly-access	Mengaktifkan akses baca saja ke wadah Amazon Elastic Container Service (ECS) dapat membantu mematuhi prinsip hak istimewa yang paling rendah. Opsi ini dapat mengurangi vektor serangan karena sistem file instance container tidak dapat dimodifikasi kecuali jika memiliki izin baca-tulis eksplisit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	ssm-document-not-p ublic	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkin kan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspo s informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	s3- bucket-acl-prohibi ted	Aturan ini memeriksa untuk melihat apakah Daftar Kontrol Akses (ACLs) digunakan untuk kontrol akses di Bucket Amazon S3. ACLs adalah mekanisme kontrol akses lama untuk bucket Amazon S3 yang AWS mendahulu i Identity and Access Management (IAM). Sebagai gantinya ACLs, ini adalah praktik terbaik untuk menggunakan kebijakan IAM atau kebijakan bucket S3 untuk mengelola akses ke bucket S3 Anda dengan lebih mudah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (A)	(A) Mengisolasi fungsi clearingh ouse perawatan kesehatan (Wajib). Jika clearinghouse perawatan kesehatan adalah bagian dari organisasi yang lebih besar, clearinghouse harus menerapka n kebijakan dan prosedur yang melindungi informasi kesehatan yang dilindungi elektroni k dari clearinghouse dari akses tidak sah oleh organisasi yang lebih besar.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (B)	(B) Otorisasi akses (Dapat dialamatkan). Menerapkan kebijakan dan prosedur untuk memberikan akses ke informasi kesehatan yang dilindungi secara elektronik, misalnya, melalui akses ke workstation, transaksi, program, proses, atau mekanisme lainnya.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (B)	(B) Otorisasi akses (Dapat dialamatkan). Menerapkan kebijakan dan prosedur untuk memberikan akses ke informasi kesehatan yang dilindungi secara elektronik, misalnya, melalui akses ke workstation, transaksi, program, proses, atau mekanisme lainnya.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (B)	(B) Otorisasi akses (Dapat dialamatkan). Menerapkan kebijakan dan prosedur untuk memberikan akses ke informasi kesehatan yang dilindungi secara elektronik, misalnya, melalui akses ke workstation, transaksi, program, proses, atau mekanisme lainnya.	access-keys-rotated	Kredensi diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (B)	(B) Otorisasi akses (Dapat dialamatkan). Menerapkan kebijakan dan prosedur untuk memberikan akses ke informasi kesehatan yang dilindungi secara elektronik, misalnya, melalui akses ke workstation, transaksi, program, proses, atau mekanisme lainnya.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (B)	(B) Otorisasi akses (Dapat dialamatkan). Menerapkan kebijakan dan prosedur untuk memberikan akses ke informasi kesehatan yang dilindungi secara elektronik, misalnya, melalui akses ke workstation, transaksi, program, proses, atau mekanisme lainnya.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (B)	(B) Otorisasi akses (Dapat dialamatkan). Menerapkan kebijakan dan prosedur untuk memberikan akses ke informasi kesehatan yang dilindungi secara elektronik, misalnya, melalui akses ke workstation, transaksi, program, proses, atau mekanisme lainnya.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensi yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (B)	(B) Otorisasi akses (Dapat dialamatkan). Menerapkan kebijakan dan prosedur untuk memberikan akses ke informasi kesehatan yang dilindungi secara elektronik, misalnya, melalui akses ke workstation, transaksi, program, proses, atau mekanisme lainnya.	secretsmanager-rotation-enabled-check	Aturan ini memastikan AWS rahasia Secrets Manager mengaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (B)	(B) Otorisasi akses (Dapat dialamatkan). Menerapkan kebijakan dan prosedur untuk memberikan akses ke informasi kesehatan yang dilindungi secara elektronik, misalnya, melalui akses ke workstation, transaksi, program, proses, atau mekanisme lainnya.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktifkan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediakan sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (B)	(B) Otorisasi akses (Dapat dialamatkan). Menerapkan kebijakan dan prosedur untuk memberikan akses ke informasi kesehatan yang dilindungi secara elektronik, misalnya, melalui akses ke workstation, transaksi, program, proses, atau mekanisme lainnya.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (B)	(B) Otorisasi akses (Dapat dialamatkan). Menerapkan kebijakan dan prosedur untuk memberikan akses ke informasi kesehatan yang dilindungi secara elektronik, misalnya, melalui akses ke workstation, transaksi, program, proses, atau mekanisme lainnya.	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi, pengembalian, dan pendelegasian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
164.308 (a) (4) (ii) (B)	(B) Otorisasi akses (Dapat dialamatkan). Menerapkan kebijakan dan prosedur untuk memberikan akses ke informasi kesehatan yang dilindungi secara elektronik, misalnya, melalui akses ke workstation, transaksi, program, proses, atau mekanisme lainnya.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (B)	(B) Otorisasi akses (Dapat dialamatkan). Menerapkan kebijakan dan prosedur untuk memberikan akses ke informasi kesehatan yang dilindungi secara elektronik, misalnya, melalui akses ke workstation, transaksi, program, proses, atau mekanisme lainnya.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
164.308 (a) (4) (ii) (B)	(B) Otorisasi akses (Dapat dialamatkan). Menerapkan kebijakan dan prosedur untuk memberikan akses ke informasi kesehatan yang dilindungi secara elektronik, misalnya, melalui akses ke workstation, transaksi, program, proses, atau mekanisme lainnya.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (B)	(B) Otorisasi akses (Dapat dialamatkan). Menerapkan kebijakan dan prosedur untuk memberikan akses ke informasi kesehatan yang dilindungi secara elektronik, misalnya, melalui akses ke workstation, transaksi, program, proses, atau mekanisme lainnya.	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (B)	(B) Otorisasi akses (Dapat dialamatkan). Menerapkan kebijakan dan prosedur untuk memberikan akses ke informasi kesehatan yang dilindungi secara elektronik, misalnya, melalui akses ke workstation, transaksi, program, proses, atau mekanisme lainnya.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (B)	(B) Otorisasi akses (Dapat dialamatkan). Menerapkan kebijakan dan prosedur untuk memberikan akses ke informasi kesehatan yang dilindungi secara elektronik, misalnya, melalui akses ke workstation, transaksi, program, proses, atau mekanisme lainnya.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.
164.308 (a) (4) (ii) (B)	(B) Otorisasi akses (Dapat dialamatkan). Menerapkan kebijakan dan prosedur untuk memberikan akses ke informasi kesehatan yang dilindungi secara elektronik, misalnya, melalui akses ke workstation, transaksi, program, proses, atau mekanisme lainnya.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (B)	(B) Otorisasi akses (Dapat dialamatkan). Menerapkan kebijakan dan prosedur untuk memberikan akses ke informasi kesehatan yang dilindungi secara elektronik, misalnya, melalui akses ke workstation, transaksi, program, proses, atau mekanisme lainnya.	ecs-containers-readonly-access	Mengaktifkan akses baca saja ke wadah Amazon Elastic Container Service (ECS) dapat membantu mematuhi prinsip hak istimewa yang paling rendah. Opsi ini dapat mengurangi vektor serangan karena sistem file instance container tidak dapat dimodifikasi kecuali jika memiliki izin baca-tulis eksplisit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (B)	(B) Otorisasi akses (Dapat dialamatkan). Menerapkan kebijakan dan prosedur untuk memberikan akses ke informasi kesehatan yang dilindungi secara elektronik, misalnya, melalui akses ke workstation, transaksi, program, proses, atau mekanisme lainnya.	s3- bucket-acl-prohibited	Aturan ini memeriksa untuk melihat apakah Daftar Kontrol Akses (ACLs) digunakan untuk kontrol akses di Bucket Amazon S3. ACLs adalah mekanisme kontrol akses lama untuk bucket Amazon S3 yang AWS mendahului Identity and Access Management (IAM). Sebagai gantinya ACLs, ini adalah praktik terbaik untuk menggunakan kebijakan IAM atau kebijakan bucket S3 untuk mengelola akses ke bucket S3 Anda dengan lebih mudah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktifkan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediakan sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi, pengembalian, dan pendelegasian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild. Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredenal masuk dalam lingkungan proyek Codebuild. AWS Gunakan OAuth alih-alih token akses pribadi atau kredensyal masuk untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	ecs-containers-readonly-access	Mengaktifkan akses baca saja ke wadah Amazon Elastic Container Service (ECS) dapat membantu mematuhi prinsip hak istimewa yang paling rendah. Opsi ini dapat mengurangi vektor serangan karena sistem file instance container tidak dapat dimodifikasi kecuali jika memiliki izin baca-tulis eksplisit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	s3- bucket-acl-prohibited	Aturan ini memeriksa untuk melihat apakah Daftar Kontrol Akses (ACLs) digunakan untuk kontrol akses di Bucket Amazon S3. ACLs adalah mekanisme kontrol akses lama untuk bucket Amazon S3 yang AWS mendahului Identity and Access Management (IAM). Sebagai gantinya ACLs, ini adalah praktik terbaik untuk menggunakan kebijakan IAM atau kebijakan bucket S3 untuk mengelola akses ke bucket S3 Anda dengan lebih mudah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (4) (ii) (C)	(C) Akses pembentukan dan modifikasi (Dapat dialamatkan). Menerapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak pengguna untuk mengakses workstation, transaksi, program, atau proses.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (5) (ii) (A)	(A) Pengingat keamanan (Dapat dialamatkan). Pembaruan keamanan berkala.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
164.308 (a) (5) (ii) (A)	(A) Pengingat keamanan (Dapat dialamatkan). Pembaruan keamanan berkala.	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (5) (ii) (A)	(A) Pengingat keamanan (Dapat dialamatkan). Pembaruan keamanan berkala.	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (5) (ii) (A)	(A) Pengingat keamanan (Dapat dialamatkan). Pembaruan keamanan berkala.	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relational Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (5) (ii) (B)	(B) Perlindungan dari perangkat lunak berbahaya (Addressable). Prosedur untuk menjaga, mendeteksi, dan melaporkan perangkat lunak berbahaya.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (5) (ii) (B)	(B) Perlindungan dari perangkat lunak berbahaya (Addressable). Prosedur untuk menjaga, mendeteksi, dan melaporkan perangkat lunak berbahaya.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (5) (ii) (B)	(B) Perlindungan dari perangkat lunak berbahaya (Addressable). Prosedur untuk menjaga, mendeteksi, dan melaporkan perangkat lunak berbahaya.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (5) (ii) (C)	(C) Pemantaua n masuk (Dapat dialamatkan). Prosedur untuk memantau upaya masuk dan melaporka n perbedaan.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (5) (ii) (C)	(C) Pemantaua n masuk (Dapat dialamatkan). Prosedur untuk memantau upaya masuk dan melaporka n perbedaan.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (5) (ii) (C)	(C) Pemantauan masuk (Dapat dialamatkan). Prosedur untuk memantau upaya masuk dan melaporkan perbedaan.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (5) (ii) (D)	(D) Manajemen kata sandi (Dapat dialamatkan). Prosedur untuk membuat, mengubah, dan melindungi kata sandi.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (6) (i)	(6) (i) Standar: Prosedur insiden keamanan. Menerapkan kebijakan dan prosedur untuk mengatasi insiden keamanan.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (6) (ii)	(ii) Spesifikasi implementasi: Respon dan Pelaporan (Wajib). Mengidentifikasi dan menanggapi insiden keamanan yang dicurigai atau diketahui; mengurangi, sejauh praktis, efek berbahaya dari insiden keamanan yang diketahui oleh entitas yang tercakup; dan mendokumentasikan insiden keamanan dan hasilnya.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (i)	(7) (i) Standar: Rencana kontinjensi. Menetapkan (dan menerapkan sesuai kebutuhan) kebijakan dan prosedur untuk menanggapi keadaan darurat atau kejadian lainnya (misalnya, kebakaran, vandalisme, kegagalan sistem, dan bencana alam) yang merusak sistem yang mengandung informasi kesehatan yang dilindungi secara elektronik.	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (i)	(7) (i) Standar: Rencana kontinjensi. Menetapkan (dan menerapkan sesuai kebutuhan) kebijakan dan prosedur untuk menanggapi keadaan darurat atau kejadian lainnya (misalnya, kebakaran, vandalisme, kegagalan sistem, dan bencana alam) yang merusak sistem yang mengandung informasi kesehatan yang dilindungi secara elektronik.	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (i)	(7) (i) Standar: Rencana kontinjensi. Menetapkan (dan menerapkan sesuai kebutuhan) kebijakan dan prosedur untuk menanggapi keadaan darurat atau kejadian lainnya (misalnya, kebakaran, vandalisme, kegagalan sistem, dan bencana alam) yang merusak sistem yang mengandung informasi kesehatan yang dilindungi secara elektronik.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (i)	(7) (i) Standar: Rencana kontinjensi. Menetapkan (dan menerapkan sesuai kebutuhan) kebijakan dan prosedur untuk menanggapi keadaan darurat atau kejadian lainnya (misalnya, kebakaran, vandalisme, kegagalan sistem, dan bencana alam) yang merusak sistem yang mengandung informasi kesehatan yang dilindungi secara elektronik.	rds-cluster-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (i)	(7) (i) Standar: Rencana kontinjensi. Menetapkan (dan menerapkan sesuai kebutuhan) kebijakan dan prosedur untuk menanggapi keadaan darurat atau kejadian lainnya (misalnya, kebakaran, vandalisme, kegagalan sistem, dan bencana alam) yang merusak sistem yang mengandung informasi kesehatan yang dilindungi secara elektronik.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) menyediakan ketersediaan dan daya tahan yang ditingkatkan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			segera setelah failover selesai.
164.308 (a) (7) (i)	(7) (i) Standar: Rencana kontinjensi. Menetapkan (dan menerapkan sesuai kebutuhan) kebijakan dan prosedur untuk menanggapi keadaan darurat atau kejadian lainnya (misalnya, kebakaran, vandalisme, kegagalan sistem, dan bencana alam) yang merusak sistem yang mengandung informasi kesehatan yang dilindungi secara elektronik.	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (i)	(7) (i) Standar: Rencana kontinjensi. Menetapkan (dan menerapkan sesuai kebutuhan) kebijakan dan prosedur untuk menanggapi keadaan darurat atau kejadian lainnya (misalnya, kebakaran, vandalisme, kegagalan sistem, dan bencana alam) yang merusak sistem yang mengandung informasi kesehatan yang dilindungi secara elektronik.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (i)	(7) (i) Standar: Rencana kontinjensi. Menetapkan (dan menerapkan sesuai kebutuhan) kebijakan dan prosedur untuk menanggapi keadaan darurat atau kejadian lainnya (misalnya, kebakaran, vandalisme, kegagalan sistem, dan bencana alam) yang merusak sistem yang mengandung informasi kesehatan yang dilindungi secara elektronik.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (i)	(7) (i) Standar: Rencana kontinjensi. Menetapkan (dan menerapkan sesuai kebutuhan) kebijakan dan prosedur untuk menanggapi keadaan darurat atau kejadian lainnya (misalnya, kebakaran, vandalisme, kegagalan sistem, dan bencana alam) yang merusak sistem yang mengandung informasi kesehatan yang dilindungi secara elektronik.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (i)	(7) (i) Standar: Rencana kontinjen si. Menetapkan (dan menerapkan sesuai kebutuhan) kebijakan dan prosedur untuk menanggapi keadaan darurat atau kejadian lainnya (misalnya, kebakaran, vandalism e, kegagalan sistem, dan bencana alam) yang merusak sistem yang mengandung informasi kesehatan yang dilindungi secara elektronik.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (i)	(7) (i) Standar: Rencana kontinjensi. Menetapkan (dan menerapkan sesuai kebutuhan) kebijakan dan prosedur untuk menanggapi keadaan darurat atau kejadian lainnya (misalnya, kebakaran, vandalisme, kegagalan sistem, dan bencana alam) yang merusak sistem yang mengandung informasi kesehatan yang dilindungi secara elektronik.	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (i)	(7) (i) Standar: Rencana kontinjensi. Menetapkan (dan menerapkan sesuai kebutuhan) kebijakan dan prosedur untuk menanggapi keadaan darurat atau kejadian lainnya (misalnya, kebakaran, vandalisme, kegagalan sistem, dan bencana alam) yang merusak sistem yang mengandung informasi kesehatan yang dilindungi secara elektronik.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (i)	(7) (i) Standar: Rencana kontinjen si. Menetapkan (dan menerapkan sesuai kebutuhan) kebijakan dan prosedur untuk menanggapi keadaan darurat atau kejadian lainnya (misalnya, kebakaran, vandalism e, kegagalan sistem, dan bencana alam) yang merusak sistem yang mengandung informasi kesehatan yang dilindungi secara elektronik.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (i)	(7) (i) Standar: Rencana kontinjensi. Menetapkan (dan menerapkan sesuai kebutuhan) kebijakan dan prosedur untuk menanggapi keadaan darurat atau kejadian lainnya (misalnya, kebakaran, vandalisme, kegagalan sistem, dan bencana alam) yang merusak sistem yang mengandung informasi kesehatan yang dilindungi secara elektronik.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (i)	(7) (i) Standar: Rencana kontinjensi. Menetapkan (dan menerapkan sesuai kebutuhan) kebijakan dan prosedur untuk menanggapi keadaan darurat atau kejadian lainnya (misalnya, kebakaran, vandalisme, kegagalan sistem, dan bencana alam) yang merusak sistem yang mengandung informasi kesehatan yang dilindungi secara elektronik.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (i)	(7) (i) Standar: Rencana kontinjensi. Menetapkan (dan menerapkan sesuai kebutuhan) kebijakan dan prosedur untuk menanggapi keadaan darurat atau kejadian lainnya (misalnya, kebakaran, vandalisme, kegagalan sistem, dan bencana alam) yang merusak sistem yang mengandung informasi kesehatan yang dilindungi secara elektronik.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (i)	(7) (i) Standar: Rencana kontinjensi. Menetapkan (dan menerapkan sesuai kebutuhan) kebijakan dan prosedur untuk menanggapi keadaan darurat atau kejadian lainnya (misalnya, kebakaran, vandalisme, kegagalan sistem, dan bencana alam) yang merusak sistem yang mengandung informasi kesehatan yang dilindungi secara elektronik.	s3- version-lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihkan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (ii) (A)	(A) Rencana pencadangan data (Diperlukan). Menetapkan dan menerapkan prosedur untuk membuat dan memelihara salinan persis informasi kesehatan yang dilindungi elektronik yang dapat diambil.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (ii) (A)	(A) Rencana pencadangan data (Diperlukan). Menetapkan dan menerapkan prosedur untuk membuat dan memelihara salinan persis informasi kesehatan yang dilindungi elektronik yang dapat diambil.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (ii) (A)	(A) Rencana pencadangan data (Diperlukan). Menetapkan dan menerapkan prosedur untuk membuat dan memelihara salinan persis informasi kesehatan yang dilindungi elektronik yang dapat diambil.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (ii) (A)	(A) Rencana pencadangan data (Diperlukan). Menetapkan dan menerapkan prosedur untuk membuat dan memelihara salinan persis informasi kesehatan yang dilindungi elektronik yang dapat diambil.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (ii) (A)	(A) Rencana pencadangan data (Diperlukan). Menetapkan dan menerapkan prosedur untuk membuat dan memelihara salinan persis informasi kesehatan yang dilindungi elektronik yang dapat diambil.	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (ii) (A)	(A) Rencana pencadangan data (Diperlukan). Menetapkan dan menerapkan prosedur untuk membuat dan memelihara salinan persis informasi kesehatan yang dilindungi elektronik yang dapat diambil.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (ii) (A)	(A) Rencana pencadangan data (Diperlukan). Menetapkan dan menerapkan prosedur untuk membuat dan memelihara salinan persis informasi kesehatan yang dilindungi elektronik yang dapat diambil.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (ii) (A)	(A) Rencana pencadangan data (Diperlukan). Menetapkan dan menerapkan prosedur untuk membuat dan memelihara salinan persis informasi kesehatan yang dilindungi elektronik yang dapat diambil.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (ii) (A)	(A) Rencana pencadangan data (Diperlukan). Menetapkan dan menerapkan prosedur untuk membuat dan memelihara salinan persis informasi kesehatan yang dilindungi elektronik yang dapat diambil.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (ii) (A)	(A) Rencana pencadangan data (Diperlukan). Menetapkan dan menerapkan prosedur untuk membuat dan memelihara salinan persis informasi kesehatan yang dilindungi elektronik yang dapat diambil.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (ii) (A)	(A) Rencana pencadangan data (Diperlukan). Menetapkan dan menerapkan prosedur untuk membuat dan memelihara salinan persis informasi kesehatan yang dilindungi elektronik yang dapat diambil.	s3- version-lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihkan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (ii) (A)	(A) Rencana pencadangan data (Diperlukan). Menetapkan dan menerapkan prosedur untuk membuat dan memelihara salinan persis informasi kesehatan yang dilindungi elektronik yang dapat diambil.	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (ii) (B)	(B) Rencana pemulihan bencana (Wajib). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk memulihkan kehilangan data.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (ii) (B)	(B) Rencana pemulihan bencana (Wajib). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk memulihkan kehilangan data.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (ii) (B)	(B) Rencana pemulihan bencana (Wajib). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk memulihkan kehilangan data.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (ii) (B)	(B) Rencana pemulihan bencana (Wajib). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk memulihkan kehilangan data.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (ii) (B)	(B) Rencana pemulihan bencana (Wajib). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk memulihkan kehilangan data.	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (ii) (B)	(B) Rencana pemulihan bencana (Wajib). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk memulihkan kehilangan data.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (ii) (B)	(B) Rencana pemulihan bencana (Wajib). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk memulihkan kehilangan data.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relational Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (ii) (B)	(B) Rencana pemulihan bencana (Wajib). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk memulihkan kehilangan data.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (ii) (B)	(B) Rencana pemulihan bencana (Wajib). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk memulihkan kehilangan data.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (ii) (B)	(B) Rencana pemulihan bencana (Wajib). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk memulihkan kehilangan data.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (ii) (B)	(B) Rencana pemulihan bencana (Wajib). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk memulihkan kehilangan data.	s3- version-lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihkan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (ii) (C)	(C) Rencana operasi mode darurat (Wajib). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk memungkin kan kelanjutan proses bisnis penting untuk perlindungan keamanan informasi kesehatan yang dilindungi elektronik saat beroperasi dalam mode darurat.	dynamodb-autoscali ng-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughpu t yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tuli s yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (ii) (C)	(C) Rencana operasi mode darurat (Wajib). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk memungkin kan kelanjutan proses bisnis penting untuk perlindungan keamanan informasi kesehatan yang dilindungi elektronik saat beroperasi dalam mode darurat.	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimba ngan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimba ngan beban lintas zona mengurang i kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkat kan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (ii) (C)	(C) Rencana operasi mode darurat (Wajib). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk memungkin kan kelanjutan proses bisnis penting untuk perlindungan keamanan informasi kesehatan yang dilindungi elektronik saat beroperasi dalam mode darurat.	elb-deletion-prote ction-enabled	Aturan ini memastika n bahwa Elastic Load Balancing memiliki perlindun gan penghapus an yang diaktifka n. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersedi aan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (ii) (C)	(C) Rencana operasi mode darurat (Wajib). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk memungkin kan kelanjutan proses bisnis penting untuk perlindungan keamanan informasi kesehatan yang dilindungi elektronik saat beroperasi dalam mode darurat.	rds-cluster-deletion-protection-diaktifkan	Pastikan instans Amazon Relationa l Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindun gan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersedi aan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (7) (ii) (C)	(C) Rencana operasi mode darurat (Wajib). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk memungkin kan kelanjutan proses bisnis penting untuk perlindungan keamanan informasi kesehatan yang dilindungi elektronik saat beroperasi dalam mode darurat.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) menyediakan ketersediaan dan daya tahan yang ditingkatkan untuk instans database. Saat Anda menyediak an instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastru ktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutk an operasi database

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			segera setelah failover selesai.
164.308 (a) (7) (ii) (C)	(C) Rencana operasi mode darurat (Wajib). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk memungkin kan kelanjutan proses bisnis penting untuk perlindungan keamanan informasi kesehatan yang dilindungi elektronik saat beroperasi dalam mode darurat.	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimpleme ntasikan untuk mencapai persyarat an ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivi tas jika salah satu koneksi Site-to-S ite VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivi tas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (8)	(8) Standar: Evaluasi. Melakukan evaluasi teknis dan nonteknis berkala, yang awalnya didasarkan pada standar yang diterapkan berdasarkan aturan ini dan selanjutnya, sebagai tanggapan terhadap perubahan lingkungan atau operasional yang mempengaruhi keamanan informasi kesehatan yang dilindungi secara elektronik, yang menetapkan sejauh mana kebijakan dan prosedur keamanan entitas memenuhi persyaratan subbagian ini.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.308 (a) (8)	(8) Standar: Evaluasi. Melakukan evaluasi teknis dan nonteknis berkala, yang awalnya didasarkan pada standar yang diterapkan berdasarkan aturan ini dan selanjutnya, sebagai tanggapan terhadap perubahan lingkungan atau operasional yang mempengaruhi keamanan informasi kesehatan yang dilindungi secara elektronik, yang menetapkan sejauh mana kebijakan dan prosedur keamanan entitas memenuhi persyaratan subbagian ini.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifka n untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	iam-user-no-policies-periksa	Aturan ini memastika n kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapka n hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	iam-user-unused-cr edentials-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCreden tialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSear ch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerluka n gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	internet-gateway-a uthorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirk an ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotens i menyebabkan degradasi ketersedi aan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	s3- account-level-publ ic-access -blok-per iodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurk an ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCES S_KEY_ID dan AWS_SECRE T_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild . Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabk an paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredenal masuk dalam lingkungan proyek Codebuild . AWS Gunakan OAuth alih-alih token akses pribadi atau kredensyal masuk untuk memberika n otorisasi untuk mengakses GitHub atau repositori Bitbucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfig urasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	ecs-containers-rea donly-access	Mengaktifkan akses baca saja ke wadah Amazon Elastic Container Service (ECS) dapat membantu mematuhi prinsip hak istimewa yang paling rendah. Opsi ini dapat mengurangi vektor serangan karena sistem file instance container tidak dapat dimodifikasi kecuali jika memiliki izin baca-tulis eksplisit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkin kan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspo s informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam 164.308 (a) (4).	s3- bucket-acl-prohibi ted	Aturan ini memeriksa untuk melihat apakah Daftar Kontrol Akses (ACLs) digunakan untuk kontrol akses di Bucket Amazon S3. ACLs adalah mekanisme kontrol akses lama untuk bucket Amazon S3 yang AWS mendahulu i Identity and Access Management (IAM). Sebagai gantinya ACLs, ini adalah praktik terbaik untuk menggunakan kebijakan IAM atau kebijakan bucket S3 untuk mengelola akses ke bucket S3 Anda dengan lebih mudah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (1)	(a) (1) Standar: Kontrol akses. Menerapkan kebijakan dan prosedur teknis untuk sistem informasi elektronik yang memelihara informasi kesehatan yang dilindungi secara elektronik untuk memungkinkan akses hanya kepada orang-orang atau program perangkat lunak yang telah diberikan hak akses sebagaima na ditentukan dalam ¤164.308 (a) (4).	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (i)	(2) Spesifikasi implementasi: (i) Identifikasi pengguna unik (Wajib). Tetapkan nama dan/atau nomor unik untuk mengident ifikasi dan melacak identitas pengguna.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (ii)	(ii) Prosedur akses darurat (Diperlukan). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk mendapatkan informasi kesehatan yang dilindung i elektronik yang diperlukan selama keadaan darurat.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (ii)	(ii) Prosedur akses darurat (Diperlukan). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk mendapatkan informasi kesehatan yang dilindung i elektronik yang diperlukan selama keadaan darurat.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (ii)	(ii) Prosedur akses darurat (Diperlukan). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk mendapatkan informasi kesehatan yang dilindung i elektronik yang diperlukan selama keadaan darurat.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (ii)	(ii) Prosedur akses darurat (Diperlukan). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk mendapatkan informasi kesehatan yang dilindung i elektronik yang diperlukan selama keadaan darurat.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (ii)	(ii) Prosedur akses darurat (Diperlukan). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk mendapatkan informasi kesehatan yang dilindung i elektronik yang diperlukan selama keadaan darurat.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (ii)	(ii) Prosedur akses darurat (Diperlukan). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk mendapatkan informasi kesehatan yang dilindung i elektronik yang diperlukan selama keadaan darurat.	dynamodb-in-backup-plan	Untuk membantu proses pencadang an data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (ii)	(ii) Prosedur akses darurat (Diperlukan). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk mendapatkan informasi kesehatan yang dilindung i elektronik yang diperlukan selama keadaan darurat.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (ii)	(ii) Prosedur akses darurat (Diperlukan). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk mendapatkan informasi kesehatan yang dilindung i elektronik yang diperlukan selama keadaan darurat.	efs-in-backup-plan	Untuk membantu proses pencadang an data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (ii)	(ii) Prosedur akses darurat (Diperlukan). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk mendapatkan informasi kesehatan yang dilindung i elektronik yang diperlukan selama keadaan darurat.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifka n untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (ii)	(ii) Prosedur akses darurat (Diperlukan). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk mendapatkan informasi kesehatan yang dilindung i elektronik yang diperlukan selama keadaan darurat.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (ii)	(ii) Prosedur akses darurat (Diperlukan). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk mendapatkan informasi kesehatan yang dilindung i elektronik yang diperlukan selama keadaan darurat.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (ii)	(ii) Prosedur akses darurat (Diperlukan). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk mendapatkan informasi kesehatan yang dilindung i elektronik yang diperlukan selama keadaan darurat.	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (ii)	(ii) Prosedur akses darurat (Diperlukan). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk mendapatkan informasi kesehatan yang dilindung i elektronik yang diperlukan selama keadaan darurat.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (ii)	(ii) Prosedur akses darurat (Diperlukan). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk mendapatkan informasi kesehatan yang dilindung i elektronik yang diperlukan selama keadaan darurat.	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.
164.312 (a) (2) (ii)	(ii) Prosedur akses darurat (Diperlukan). Menetapkan (dan menerapkan sesuai kebutuhan) prosedur untuk mendapatkan informasi kesehatan yang dilindung i elektronik yang diperlukan selama keadaan darurat.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (iv)	(iv) Enkripsi dan dekripsi (Dapat dialamatkan). Menerapkan mekanisme untuk mengenkripsi dan mendekripsi informasi kesehatan yang dilindungi secara elektronik.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
164.312 (a) (2) (iv)	(iv) Enkripsi dan dekripsi (Dapat dialamatkan). Menerapkan mekanisme untuk mengenkripsi dan mendekripsi informasi kesehatan yang dilindungi secara elektronik.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (iv)	(iv) Enkripsi dan dekripsi (Dapat dialamatkan). Menerapkan mekanisme untuk mengenkripsi dan mendekripsi informasi kesehatan yang dilindungi secara elektronik.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrai l jejak Anda.
164.312 (a) (2) (iv)	(iv) Enkripsi dan dekripsi (Dapat dialamatkan). Menerapkan mekanisme untuk mengenkripsi dan mendekripsi informasi kesehatan yang dilindungi secara elektronik.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (iv)	(iv) Enkripsi dan dekripsi (Dapat dialamatkan). Menerapkan mekanisme untuk mengenkripsi dan mendekripsi informasi kesehatan yang dilindungi secara elektronik.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
164.312 (a) (2) (iv)	(iv) Enkripsi dan dekripsi (Dapat dialamatkan). Menerapkan mekanisme untuk mengenkripsi dan mendekripsi informasi kesehatan yang dilindungi secara elektronik.	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (iv)	(iv) Enkripsi dan dekripsi (Dapat dialamatkan). Menerapkan mekanisme untuk mengenkripsi dan mendekripsi informasi kesehatan yang dilindungi secara elektronik.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (iv)	(iv) Enkripsi dan dekripsi (Dapat dialamatkan). Menerapkan mekanisme untuk mengenkripsi dan mendekripsi informasi kesehatan yang dilindungi secara elektronik.	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (iv)	(iv) Enkripsi dan dekripsi (Dapat dialamatkan). Menerapkan mekanisme untuk mengenkripsi dan mendekripsi informasi kesehatan yang dilindungi secara elektronik.	elb-predefined-security-policy-ssl-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa pendengar SSL Classic Elastic Load Balancing Anda menggunakan kebijakan keamanan yang telah ditentukan sebelumnya. Elastic Load Balancing menyediakan konfigurasi negosiasi SSL yang telah ditentukan sebelumnya yang digunakan untuk negosiasi SSL ketika koneksi dibuat antara klien dan penyeimbang beban Anda. Konfigurasi negosiasi SSL memberikan kompatibilitas dengan berbagai klien dan menggunakan algoritma kriptografi berkekuatan tinggi. Aturan ini mengharuskan Anda menetapkan kebijakan keamanan yang telah ditentuka

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			n untuk pendengar SSL Anda. Kebijakan keamanan default adalah: ELBSecurity Policy-TLS-1-2-2017-0. Nilai aktual harus mencerminkan kebijakan organisasi Anda
164.312 (a) (2) (iv)	(iv) Enkripsi dan dekripsi (Dapat dialamatkan). Menerapkan mekanisme untuk mengenkripsi dan mendekripsi informasi kesehatan yang dilindungi secara elektronik.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
164.312 (a) (2) (iv)	(iv) Enkripsi dan dekripsi (Dapat dialamatkan). Menerapkan mekanisme untuk mengenkripsi dan mendekripsi informasi kesehatan yang dilindungi secara elektronik.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (iv)	(iv) Enkripsi dan dekripsi (Dapat dialamatkan). Menerapkan mekanisme untuk mengenkripsi dan mendekripsi informasi kesehatan yang dilindungi secara elektronik.	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
164.312 (a) (2) (iv)	(iv) Enkripsi dan dekripsi (Dapat dialamatkan). Menerapkan mekanisme untuk mengenkripsi dan mendekripsi informasi kesehatan yang dilindungi secara elektronik.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (iv)	(iv) Enkripsi dan dekripsi (Dapat dialamatkan). Menerapkan mekanisme untuk mengenkripsi dan mendekripsi informasi kesehatan yang dilindungi secara elektronik.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (iv)	(iv) Enkripsi dan dekripsi (Dapat dialamatkan). Menerapkan mekanisme untuk mengenkripsi dan mendekripsi informasi kesehatan yang dilindungi secara elektronik.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
164.312 (a) (2) (iv)	(iv) Enkripsi dan dekripsi (Dapat dialamatkan). Menerapkan mekanisme untuk mengenkripsi dan mendekripsi informasi kesehatan yang dilindungi secara elektronik.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (iv)	(iv) Enkripsi dan dekripsi (Dapat dialamatkan). Menerapkan mekanisme untuk mengenkripsi dan mendekripsi informasi kesehatan yang dilindungi secara elektronik.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
164.312 (a) (2) (iv)	(iv) Enkripsi dan dekripsi (Dapat dialamatkan). Menerapkan mekanisme untuk mengenkripsi dan mendekripsi informasi kesehatan yang dilindungi secara elektronik.	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (iv)	(iv) Enkripsi dan dekripsi (Dapat dialamatkan). Menerapkan mekanisme untuk mengenkripsi dan mendekripsi informasi kesehatan yang dilindungi secara elektronik.	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
164.312 (a) (2) (iv)	(iv) Enkripsi dan dekripsi (Dapat dialamatkan). Menerapkan mekanisme untuk mengenkripsi dan mendekripsi informasi kesehatan yang dilindungi secara elektronik.	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (iv)	(iv) Enkripsi dan dekripsi (Dapat dialamatkan). Menerapkan mekanisme untuk mengenkripsi dan mendekripsi informasi kesehatan yang dilindungi secara elektronik.	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (iv)	(iv) Enkripsi dan dekripsi (Dapat dialamatkan). Menerapkan mekanisme untuk mengenkripsi dan mendekripsi informasi kesehatan yang dilindungi secara elektronik.	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
164.312 (a) (2) (iv)	(iv) Enkripsi dan dekripsi (Dapat dialamatkan). Menerapkan mekanisme untuk mengenkripsi dan mendekripsi informasi kesehatan yang dilindungi secara elektronik.	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (iv)	(iv) Enkripsi dan dekripsi (Dapat dialamatkan). Menerapkan mekanisme untuk mengenkripsi dan mendekripsi informasi kesehatan yang dilindungi secara elektronik.	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
164.312 (a) (2) (iv)	(iv) Enkripsi dan dekripsi (Dapat dialamatkan). Menerapkan mekanisme untuk mengenkripsi dan mendekripsi informasi kesehatan yang dilindungi secara elektronik.	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (a) (2) (iv)	(iv) Enkripsi dan dekripsi (Dapat dialamatkan). Menerapkan mekanisme untuk mengenkripsi dan mendekripsi informasi kesehatan yang dilindungi secara elektronik.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
164.312 (a) (2) (iv)	(iv) Enkripsi dan dekripsi (Dapat dialamatkan). Menerapkan mekanisme untuk mengenkripsi dan mendekripsi informasi kesehatan yang dilindungi secara elektronik.	kinesis-stream-encrypted	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (b)	(b) Standar: Kontrol audit. Menerapkan perangkat keras, perangkat lunak, dan/atau mekanisme prosedural yang mencatat dan memeriksa aktivitas dalam sistem informasi yang berisi atau menggunakan informasi kesehatan yang dilindungi secara elektronik.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (b)	(b) Standar: Kontrol audit. Menerapkan perangkat keras, perangkat lunak, dan/atau mekanisme prosedural yang mencatat dan memeriksa aktivitas dalam sistem informasi yang berisi atau menggunakan informasi kesehatan yang dilindungi secara elektronik.	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (b)	(b) Standar: Kontrol audit. Menerapkan perangkat keras, perangkat lunak, dan/atau mekanisme prosedural yang mencatat dan memeriksa aktivitas dalam sistem informasi yang berisi atau menggunakan informasi kesehatan yang dilindungi secara elektronik.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
164.312 (b)	(b) Standar: Kontrol audit. Menerapkan perangkat keras, perangkat lunak, dan/atau mekanisme prosedural yang mencatat dan memeriksa aktivitas dalam sistem informasi yang berisi atau menggunakan informasi kesehatan yang dilindungi secara elektronik.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (b)	(b) Standar: Kontrol audit. Menerapkan perangkat keras, perangkat lunak, dan/atau mekanisme prosedural yang mencatat dan memeriksa aktivitas dalam sistem informasi yang berisi atau menggunakan informasi kesehatan yang dilindungi secara elektronik.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (b)	(b) Standar: Kontrol audit. Menerapkan perangkat keras, perangkat lunak, dan/atau mekanisme prosedural yang mencatat dan memeriksa aktivitas dalam sistem informasi yang berisi atau menggunakan informasi kesehatan yang dilindungi secara elektronik.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (b)	(b) Standar: Kontrol audit. Menerapkan perangkat keras, perangkat lunak, dan/atau mekanisme prosedural yang mencatat dan memeriksa aktivitas dalam sistem informasi yang berisi atau menggunakan informasi kesehatan yang dilindungi secara elektronik.	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
164.312 (b)	(b) Standar: Kontrol audit. Menerapkan perangkat keras, perangkat lunak, dan/atau mekanisme prosedural yang mencatat dan memeriksa aktivitas dalam sistem informasi yang berisi atau menggunakan informasi kesehatan yang dilindungi secara elektronik.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (b)	(b) Standar: Kontrol audit. Menerapkan perangkat keras, perangkat lunak, dan/atau mekanisme prosedural yang mencatat dan memeriksa aktivitas dalam sistem informasi yang berisi atau menggunakan informasi kesehatan yang dilindungi secara elektronik.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (b)	(b) Standar: Kontrol audit. Menerapkan perangkat keras, perangkat lunak, dan/atau mekanisme prosedural yang mencatat dan memeriksa aktivitas dalam sistem informasi yang berisi atau menggunakan informasi kesehatan yang dilindungi secara elektronik.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (b)	(b) Standar: Kontrol audit. Menerapkan perangkat keras, perangkat lunak, dan/atau mekanisme prosedural yang mencatat dan memeriksa aktivitas dalam sistem informasi yang berisi atau menggunakan informasi kesehatan yang dilindungi secara elektronik.	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (b)	(b) Standar: Kontrol audit. Menerapkan perangkat keras, perangkat lunak, dan/atau mekanisme prosedural yang mencatat dan memeriksa aktivitas dalam sistem informasi yang berisi atau menggunakan informasi kesehatan yang dilindungi secara elektronik.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (b)	(b) Standar: Kontrol audit. Menerapkan perangkat keras, perangkat lunak, dan/atau mekanisme prosedural yang mencatat dan memeriksa aktivitas dalam sistem informasi yang berisi atau menggunakan informasi kesehatan yang dilindungi secara elektronik.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (b)	(b) Standar: Kontrol audit. Menerapkan perangkat keras, perangkat lunak, dan/atau mekanisme prosedural yang mencatat dan memeriksa aktivitas dalam sistem informasi yang berisi atau menggunakan informasi kesehatan yang dilindungi secara elektronik.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (b)	(b) Standar: Kontrol audit. Menerapkan perangkat keras, perangkat lunak, dan/atau mekanisme prosedural yang mencatat dan memeriksa aktivitas dalam sistem informasi yang berisi atau menggunakan informasi kesehatan yang dilindungi secara elektronik.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (b)	(b) Standar: Kontrol audit. Menerapkan perangkat keras, perangkat lunak, dan/atau mekanisme prosedural yang mencatat dan memeriksa aktivitas dalam sistem informasi yang berisi atau menggunakan informasi kesehatan yang dilindungi secara elektronik.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (b)	(b) Standar: Kontrol audit. Menerapkan perangkat keras, perangkat lunak, dan/atau mekanisme prosedural yang mencatat dan memeriksa aktivitas dalam sistem informasi yang berisi atau menggunakan informasi kesehatan yang dilindungi secara elektronik.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (b)	(b) Standar: Kontrol audit. Menerapkan perangkat keras, perangkat lunak, dan/atau mekanisme prosedural yang mencatat dan memeriksa aktivitas dalam sistem informasi yang berisi atau menggunakan informasi kesehatan yang dilindungi secara elektronik.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (b)	(b) Standar: Kontrol audit. Menerapkan perangkat keras, perangkat lunak, dan/atau mekanisme prosedural yang mencatat dan memeriksa aktivitas dalam sistem informasi yang berisi atau menggunakan informasi kesehatan yang dilindungi secara elektronik.	s3- event-notifications-enabled	Pemberitahuan peristiwa Amazon S3 dapat memberi tahu personel terkait tentang modifikasi yang tidak disengaja atau disengaja pada objek bucket Anda. Contoh peringatan meliputi: objek baru adalah pembuatan, penghapusan objek, restorasi objek, objek yang hilang dan direplikasi.
164.312 (b)	(b) Standar: Kontrol audit. Menerapkan perangkat keras, perangkat lunak, dan/atau mekanisme prosedural yang mencatat dan memeriksa aktivitas dalam sistem informasi yang berisi atau menggunakan informasi kesehatan yang dilindungi secara elektronik.	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (c) (1)	(c) (1) Standar: Integritas. Menerapkan kebijakan dan prosedur untuk melindungi informasi kesehatan yang dilindungi secara elektronik dari perubahan atau kerusakan yang tidak tepat.	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (c) (1)	(c) (1) Standar: Integritas. Menerapkan kebijakan dan prosedur untuk melindungi informasi kesehatan yang dilindungi secara elektronik dari perubahan atau kerusakan yang tidak tepat.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (c) (1)	(c) (1) Standar: Integritas. Menerapkan kebijakan dan prosedur untuk melindungi informasi kesehatan yang dilindungi secara elektronik dari perubahan atau kerusakan yang tidak tepat.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (c) (1)	(c) (1) Standar: Integritas. Menerapkan kebijakan dan prosedur untuk melindungi informasi kesehatan yang dilindungi secara elektronik dari perubahan atau kerusakan yang tidak tepat.	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
164.312 (c) (1)	(c) (1) Standar: Integritas. Menerapkan kebijakan dan prosedur untuk melindungi informasi kesehatan yang dilindungi secara elektronik dari perubahan atau kerusakan yang tidak tepat.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (c) (2)	(2) Spesifikasi implementasi: Mekanisme untuk mengautentikasi informasi kesehatan yang dilindungi secara elektronik (Dapat dialamatkan). Menerapkan mekanisme elektronik untuk menguatkan bahwa informasi kesehatan yang dilindungi secara elektronik belum diubah atau dihancurkan dengan cara yang tidak sah.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (c) (2)	(2) Spesifikasi implementasi: Mekanisme untuk mengautentikasi informasi kesehatan yang dilindungi secara elektronik (Dapat dialamatkan). Menerapkan mekanisme elektronik untuk menguatkan bahwa informasi kesehatan yang dilindungi secara elektronik belum diubah atau dihancurkan dengan cara yang tidak sah.	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (c) (2)	(2) Spesifikasi implementasi: Mekanisme untuk mengautentikasi informasi kesehatan yang dilindungi secara elektronik (Dapat dialamatkan). Menerapkan mekanisme elektronik untuk menguatkan bahwa informasi kesehatan yang dilindungi secara elektronik belum diubah atau dihancurkan dengan cara yang tidak sah.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (c) (2)	(2) Spesifikasi implementasi: Mekanisme untuk mengautentikasi informasi kesehatan yang dilindungi secara elektronik (Dapat dialamatkan). Menerapkan mekanisme elektronik untuk menguatkan bahwa informasi kesehatan yang dilindungi secara elektronik belum diubah atau dihancurkan dengan cara yang tidak sah.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (c) (2)	(2) Spesifikasi implementasi: Mekanisme untuk mengautentikasi informasi kesehatan yang dilindungi secara elektronik (Dapat dialamatkan). Menerapkan mekanisme elektronik untuk menguatkan bahwa informasi kesehatan yang dilindungi secara elektronik belum diubah atau dihancurkan dengan cara yang tidak sah.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (d)	(d) Standar: Otentikasi orang atau entitas. Menerapkan prosedur untuk memverifikasi bahwa seseorang atau entitas yang mencari akses ke informasi kesehatan yang dilindungi elektronik adalah yang diklaim.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (d)	(d) Standar: Otentikasi orang atau entitas. Menerapkan prosedur untuk memverifikasi bahwa seseorang atau entitas yang mencari akses ke informasi kesehatan yang dilindungi elektronik adalah yang diklaim.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (d)	(d) Standar: Otentikasi orang atau entitas. Menerapkan prosedur untuk memverifikasi bahwa seseorang atau entitas yang mencari akses ke informasi kesehatan yang dilindungi elektronik adalah yang diklaim.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (d)	(d) Standar: Otentikasi orang atau entitas. Menerapkan prosedur untuk memverifikasi bahwa seseorang atau entitas yang mencari akses ke informasi kesehatan yang dilindungi elektronik adalah yang diklaim.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (d)	(d) Standar: Otentikasi orang atau entitas. Menerapkan prosedur untuk memverifikasi bahwa seseorang atau entitas yang mencari akses ke informasi kesehatan yang dilindungi elektronik adalah yang diklaim.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	elb-predefined-security-policy-ssl-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa pendengar SSL Classic Elastic Load Balancing Anda menggunakan kebijakan keamanan yang telah ditentukan sebelumnya. Elastic Load Balancing menyediakan konfigurasi negosiasi SSL yang telah ditentukan sebelumnya yang digunakan untuk negosiasi SSL ketika koneksi dibuat antara klien dan penyeimbang beban Anda. Konfigurasi negosiasi SSL memberikan kompatibilitas dengan berbagai klien dan menggunakan algoritma kriptografi berkekuatan tinggi. Aturan ini mengharuskan Anda menetapkan kebijakan keamanan yang telah ditentuka

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			n untuk pendengar SSL Anda. Kebijakan keamanan default adalah: ELBSecurity Policy-TLS-1-2-2017-0. Nilai aktual harus mencerminkan kebijakan organisasi Anda
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindunginya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (1)	(e) (1) Standar: Keamanan transmisi. Menerapkan langkah-langkah keamanan teknis untuk menjaga terhadap akses tidak sah ke informasi kesehatan yang dilindungi elektronik yang sedang dikirimkan melalui jaringan komunikasi elektronik.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
164.312 (e) (2) (i)	(i) Kontrol integritas (Dapat dialamatkan). Menerapkan langkah-langkah keamanan untuk memastikan bahwa informasi kesehatan yang dilindungi elektronik yang ditransmisikan secara elektronik tidak dimodifikasi secara tidak benar tanpa deteksi sampai dibuang.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (2) (i)	(i) Kontrol integritas (Dapat dialamatkan). Menerapkan langkah-langkah keamanan untuk memastika n bahwa informasi kesehatan yang dilindungi elektronik yang ditransmisikan secara elektronik tidak dimodifikasi secara tidak benar tanpa deteksi sampai dibuang.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
164.312 (e) (2) (i)	(i) Kontrol integritas (Dapat dialamatkan). Menerapkan langkah-langkah keamanan untuk memastika n bahwa informasi kesehatan yang dilindungi elektronik yang ditransmisikan secara elektronik tidak dimodifikasi secara tidak benar tanpa deteksi sampai dibuang.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-n ode enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkrip si memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (2) (i)	(i) Kontrol integritas (Dapat dialamatkan). Menerapkan langkah-langkah keamanan untuk memastika n bahwa informasi kesehatan yang dilindungi elektronik yang ditransmisikan secara elektronik tidak dimodifikasi secara tidak benar tanpa deteksi sampai dibuang.	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (2) (i)	(i) Kontrol integritas (Dapat dialamatkan). Menerapkan langkah-langkah keamanan untuk memastikan bahwa informasi kesehatan yang dilindungi elektronik yang ditransmisikan secara elektronik tidak dimodifikasi secara tidak benar tanpa deteksi sampai dibuang.	elb-predefined-security-policy-ssl-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa pendengar SSL Classic Elastic Load Balancing Anda menggunakan kebijakan keamanan yang telah ditentukan sebelumnya. Elastic Load Balancing menyediakan konfigurasi negosiasi SSL yang telah ditentukan sebelumnya yang digunakan untuk negosiasi SSL ketika koneksi dibuat antara klien dan penyeimbang beban Anda. Konfigurasi negosiasi SSL memberikan kompatibilitas dengan berbagai klien dan menggunakan algoritma kriptografi berkekuatan tinggi. Aturan ini mengharuskan Anda menetapkan kebijakan keamanan yang telah ditentuka

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			n untuk pendengar SSL Anda. Kebijakan keamanan default adalah: ELBSecurity Policy-TLS-1-2-2017-0. Nilai aktual harus mencerminkan kebijakan organisasi Anda
164.312 (e) (2) (i)	(i) Kontrol integritas (Dapat dialamatkan). Menerapkan langkah-langkah keamanan untuk memastikan bahwa informasi kesehatan yang dilindungi elektronik yang ditransmisikan secara elektronik tidak dimodifikasi secara tidak benar tanpa deteksi sampai dibuang.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (2) (i)	(i) Kontrol integritas (Dapat dialamatkan). Menerapkan langkah-langkah keamanan untuk memastika n bahwa informasi kesehatan yang dilindungi elektronik yang ditransmisikan secara elektronik tidak dimodifikasi secara tidak benar tanpa deteksi sampai dibuang.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
164.312 (e) (2) (i)	(i) Kontrol integritas (Dapat dialamatkan). Menerapkan langkah-langkah keamanan untuk memastika n bahwa informasi kesehatan yang dilindungi elektronik yang ditransmisikan secara elektronik tidak dimodifikasi secara tidak benar tanpa deteksi sampai dibuang.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (2) (i)	(i) Kontrol integritas (Dapat dialamatkan). Menerapkan langkah-langkah keamanan untuk memastikan bahwa informasi kesehatan yang dilindungi elektronik yang ditransmisikan secara elektronik tidak dimodifikasi secara tidak benar tanpa deteksi sampai dibuang.	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
164.312 (e) (2) (i)	(i) Kontrol integritas (Dapat dialamatkan). Menerapkan langkah-langkah keamanan untuk memastikan bahwa informasi kesehatan yang dilindungi elektronik yang ditransmisikan secara elektronik tidak dimodifikasi secara tidak benar tanpa deteksi sampai dibuang.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (2) (ii)	(ii) Enkripsi (Dapat Dialamatkan). Menerapkan mekanisme untuk mengenkripsi informasi kesehatan yang dilindungi secara elektronik kapan pun dianggap tepat.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
164.312 (e) (2) (ii)	(ii) Enkripsi (Dapat Dialamatkan). Menerapkan mekanisme untuk mengenkripsi informasi kesehatan yang dilindungi secara elektronik kapan pun dianggap tepat.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (2) (ii)	(ii) Enkripsi (Dapat Dialamatkan). Menerapkan mekanisme untuk mengenkripsi informasi kesehatan yang dilindungi secara elektronik kapan pun dianggap tepat.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrai l jejak Anda.
164.312 (e) (2) (ii)	(ii) Enkripsi (Dapat Dialamatkan). Menerapkan mekanisme untuk mengenkripsi informasi kesehatan yang dilindungi secara elektronik kapan pun dianggap tepat.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
164.312 (e) (2) (ii)	(ii) Enkripsi (Dapat Dialamatkan). Menerapkan mekanisme untuk mengenkripsi informasi kesehatan yang dilindungi secara elektronik kapan pun dianggap tepat.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (2) (ii)	(ii) Enkripsi (Dapat Dialamatkan). Menerapkan mekanisme untuk mengenkripsi informasi kesehatan yang dilindungi secara elektronik kapan pun dianggap tepat.	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
164.312 (e) (2) (ii)	(ii) Enkripsi (Dapat Dialamatkan). Menerapkan mekanisme untuk mengenkripsi informasi kesehatan yang dilindungi secara elektronik kapan pun dianggap tepat.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (2) (ii)	(ii) Enkripsi (Dapat Dialamatkan). Menerapkan mekanisme untuk mengenkripsi informasi kesehatan yang dilindungi secara elektronik kapan pun dianggap tepat.	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (2) (ii)	(ii) Enkripsi (Dapat Dialamatkan). Menerapkan mekanisme untuk mengenkripsi informasi kesehatan yang dilindungi secara elektronik kapan pun dianggap tepat.	elb-predefined-security-policy-ssl-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa pendengar SSL Classic Elastic Load Balancing Anda menggunakan kebijakan keamanan yang telah ditentukan sebelumnya. Elastic Load Balancing menyediakan konfigurasi negosiasi SSL yang telah ditentukan sebelumnya yang digunakan untuk negosiasi SSL ketika koneksi dibuat antara klien dan penyeimbang beban Anda. Konfigurasi negosiasi SSL memberikan kompatibilitas dengan berbagai klien dan menggunakan algoritma kriptografi berkekuatan tinggi. Aturan ini mengharuskan Anda menetapkan kebijakan keamanan yang telah ditentuka

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			n untuk pendengar SSL Anda. Kebijakan keamanan default adalah: ELBSecurity Policy-TLS-1-2-2017-0. Nilai aktual harus mencerminkan kebijakan organisasi Anda
164.312 (e) (2) (ii)	(ii) Enkripsi (Dapat Dialamatkan). Menerapkan mekanisme untuk mengenkripsi informasi kesehatan yang dilindungi secara elektronik kapan pun dianggap tepat.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
164.312 (e) (2) (ii)	(ii) Enkripsi (Dapat Dialamatkan). Menerapkan mekanisme untuk mengenkripsi informasi kesehatan yang dilindungi secara elektronik kapan pun dianggap tepat.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (2) (ii)	(ii) Enkripsi (Dapat Dialamatkan). Menerapkan mekanisme untuk mengenkripsi informasi kesehatan yang dilindungi secara elektronik kapan pun dianggap tepat.	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
164.312 (e) (2) (ii)	(ii) Enkripsi (Dapat Dialamatkan). Menerapkan mekanisme untuk mengenkripsi informasi kesehatan yang dilindungi secara elektronik kapan pun dianggap tepat.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (2) (ii)	(ii) Enkripsi (Dapat Dialamatkan). Menerapkan mekanisme untuk mengenkripsi informasi kesehatan yang dilindungi secara elektronik kapan pun dianggap tepat.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (2) (ii)	(ii) Enkripsi (Dapat Dialamatkan). Menerapkan mekanisme untuk mengenkripsi informasi kesehatan yang dilindungi secara elektronik kapan pun dianggap tepat.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
164.312 (e) (2) (ii)	(ii) Enkripsi (Dapat Dialamatkan). Menerapkan mekanisme untuk mengenkripsi informasi kesehatan yang dilindungi secara elektronik kapan pun dianggap tepat.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (2) (ii)	(ii) Enkripsi (Dapat Dialamatkan). Menerapkan mekanisme untuk mengenkripsi informasi kesehatan yang dilindungi secara elektronik kapan pun dianggap tepat.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
164.312 (e) (2) (ii)	(ii) Enkripsi (Dapat Dialamatkan). Menerapkan mekanisme untuk mengenkripsi informasi kesehatan yang dilindungi secara elektronik kapan pun dianggap tepat.	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (2) (ii)	(ii) Enkripsi (Dapat Dialamatkan). Menerapkan mekanisme untuk mengenkripsi informasi kesehatan yang dilindungi secara elektronik kapan pun dianggap tepat.	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
164.312 (e) (2) (ii)	(ii) Enkripsi (Dapat Dialamatkan). Menerapkan mekanisme untuk mengenkripsi informasi kesehatan yang dilindungi secara elektronik kapan pun dianggap tepat.	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (2) (ii)	(ii) Enkripsi (Dapat Dialamatkan). Menerapkan mekanisme untuk mengenkripsi informasi kesehatan yang dilindungi secara elektronik kapan pun dianggap tepat.	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (2) (ii)	(ii) Enkripsi (Dapat Dialamatkan). Menerapkan mekanisme untuk mengenkripsi informasi kesehatan yang dilindungi secara elektronik kapan pun dianggap tepat.	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
164.312 (e) (2) (ii)	(ii) Enkripsi (Dapat Dialamatkan). Menerapkan mekanisme untuk mengenkripsi informasi kesehatan yang dilindungi secara elektronik kapan pun dianggap tepat.	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (2) (ii)	(ii) Enkripsi (Dapat Dialamatkan). Menerapkan mekanisme untuk mengenkripsi informasi kesehatan yang dilindungi secara elektronik kapan pun dianggap tepat.	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
164.312 (e) (2) (ii)	(ii) Enkripsi (Dapat Dialamatkan). Menerapkan mekanisme untuk mengenkripsi informasi kesehatan yang dilindungi secara elektronik kapan pun dianggap tepat.	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.312 (e) (2) (ii)	(ii) Enkripsi (Dapat Dialamatkan). Menerapkan mekanisme untuk mengenkripsi informasi kesehatan yang dilindungi secara elektronik kapan pun dianggap tepat.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
164.312 (e) (2) (ii)	(ii) Enkripsi (Dapat Dialamatkan). Menerapkan mekanisme untuk mengenkripsi informasi kesehatan yang dilindungi secara elektronik kapan pun dianggap tepat.	kinesis-stream-encrypted	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (1)	(b) (1) Standar: Persyaratan untuk rencana kesehatan kelompok. Kecuali jika satu-satunya informasi kesehatan yang dilindungi secara elektronik yang diungkapkan kepada sponsor rencana diungkapkan sesuai dengan ¤164.504 (f) (1) (ii) atau (iii), atau sebagaimana diizinkan berdasark an ¤164.508, rencana kesehatan kelompok harus memastikan bahwa dokumen rencanany a menyatakan bahwa sponsor rencana akan secara wajar dan tepat melindung i informasi kesehatan yang dilindung i elektronik yang dibuat, diterima, dipelihara, atau dikirimkan ke atau oleh sponsor rencana atas nama rencana kesehatan kelompok.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrai l jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (1)	(b) (1) Standar: Persyaratan untuk rencana kesehatan kelompok. Kecuali jika satu-satunya informasi kesehatan yang dilindungi secara elektronik yang diungkapkan kepada sponsor rencana diungkapkan sesuai dengan ¤164.504 (f) (1) (ii) atau (iii), atau sebagaimana diizinkan berdasark an ¤164.508, rencana kesehatan kelompok harus memastikan bahwa dokumen rencanany a menyatakan bahwa sponsor rencana akan secara wajar dan tepat melindung i informasi kesehatan yang dilindung i elektronik yang dibuat, diterima, dipelihara, atau dikirimkan ke atau oleh sponsor rencana atas nama rencana kesehatan kelompok.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (1)	(b) (1) Standar: Persyaratan untuk rencana kesehatan kelompok. Kecuali jika satu-satunya informasi kesehatan yang dilindungi secara elektronik yang diungkapkan kepada sponsor rencana diungkapkan sesuai dengan ¤164.504 (f) (1) (ii) atau (iii), atau sebagaimana diizinkan berdasarkan ¤164.508, rencana kesehatan kelompok harus memastikan bahwa dokumen rencananya menyatakan bahwa sponsor rencana akan secara wajar dan tepat melindungi informasi kesehatan yang dilindungi elektronik yang dibuat, diterima, dipelihara, atau dikirimkan ke atau oleh sponsor rencana atas nama rencana kesehatan kelompok.	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (1)	(b) (1) Standar: Persyaratan untuk rencana kesehatan kelompok. Kecuali jika satu-satunya informasi kesehatan yang dilindungi secara elektronik yang diungkapkan kepada sponsor rencana diungkapkan sesuai dengan ¤164.504 (f) (1) (ii) atau (iii), atau sebagaimana diizinkan berdasarkan ¤164.508, rencana kesehatan kelompok harus memastikan bahwa dokumen rencananya menyatakan bahwa sponsor rencana akan secara wajar dan tepat melindungi informasi kesehatan yang dilindungi elektronik yang dibuat, diterima, dipelihara, atau dikirimkan ke atau oleh sponsor rencana atas nama rencana kesehatan kelompok.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (1)	(b) (1) Standar: Persyaratan untuk rencana kesehatan kelompok. Kecuali jika satu-satunya informasi kesehatan yang dilindungi secara elektronik yang diungkapkan kepada sponsor rencana diungkapkan sesuai dengan ¤164.504 (f) (1) (ii) atau (iii), atau sebagaimana diizinkan berdasark an ¤164.508, rencana kesehatan kelompok harus memastikan bahwa dokumen rencanany a menyatakan bahwa sponsor rencana akan secara wajar dan tepat melindung i informasi kesehatan yang dilindung i elektronik yang dibuat, diterima, dipelihara, atau dikirimkan ke atau oleh sponsor rencana atas nama rencana kesehatan kelompok.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (1)	(b) (1) Standar: Persyaratan untuk rencana kesehatan kelompok. Kecuali jika satu-satunya informasi kesehatan yang dilindungi secara elektronik yang diungkapkan kepada sponsor rencana diungkapkan sesuai dengan ¤164.504 (f) (1) (ii) atau (iii), atau sebagaimana diizinkan berdasark an ¤164.508, rencana kesehatan kelompok harus memastikan bahwa dokumen rencanany a menyatakan bahwa sponsor rencana akan secara wajar dan tepat melindung i informasi kesehatan yang dilindung i elektronik yang dibuat, diterima, dipelihara, atau dikirimkan ke atau oleh sponsor rencana atas nama rencana kesehatan kelompok.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (1)	(b) (1) Standar: Persyaratan untuk rencana kesehatan kelompok. Kecuali jika satu-satunya informasi kesehatan yang dilindungi secara elektronik yang diungkapkan kepada sponsor rencana diungkapkan sesuai dengan ¤164.504 (f) (1) (ii) atau (iii), atau sebagaimana diizinkan berdasarkan ¤164.508, rencana kesehatan kelompok harus memastikan bahwa dokumen rencananya menyatakan bahwa sponsor rencana akan secara wajar dan tepat melindungi informasi kesehatan yang dilindungi elektronik yang dibuat, diterima, dipelihara, atau dikirimkan ke atau oleh sponsor rencana atas nama rencana kesehatan kelompok.	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (1)	(b) (1) Standar: Persyaratan untuk rencana kesehatan kelompok. Kecuali jika satu-satunya informasi kesehatan yang dilindungi secara elektronik yang diungkapkan kepada sponsor rencana diungkapkan sesuai dengan ¤164.504 (f) (1) (ii) atau (iii), atau sebagaimana diizinkan berdasarkan ¤164.508, rencana kesehatan kelompok harus memastikan bahwa dokumen rencananya menyatakan bahwa sponsor rencana akan secara wajar dan tepat melindungi informasi kesehatan yang dilindungi elektronik yang dibuat, diterima, dipelihara, atau dikirimkan ke atau oleh sponsor rencana atas nama rencana kesehatan kelompok.	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (1)	(b) (1) Standar: Persyaratan untuk rencana kesehatan kelompok. Kecuali jika satu-satunya informasi kesehatan yang dilindungi secara elektronik yang diungkapkan kepada sponsor rencana diungkapkan sesuai dengan ¤164.504 (f) (1) (ii) atau (iii), atau sebagaimana diizinkan berdasark an ¤164.508, rencana kesehatan kelompok harus memastikan bahwa dokumen rencanany a menyatakan bahwa sponsor rencana akan secara wajar dan tepat melindung i informasi kesehatan yang dilindung i elektronik yang dibuat, diterima, dipelihara, atau dikirimkan ke atau oleh sponsor rencana atas nama rencana kesehatan kelompok.	opensearch-node-to -node-pemeriksaan enkripsi-	Pastikan node-to-n ode enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkrip si memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (1)	(b) (1) Standar: Persyaratan untuk rencana kesehatan kelompok. Kecuali jika satu-satunya informasi kesehatan yang dilindungi secara elektronik yang diungkapkan kepada sponsor rencana diungkapkan sesuai dengan ¤164.504 (f) (1) (ii) atau (iii), atau sebagaimana diizinkan berdasark an ¤164.508, rencana kesehatan kelompok harus memastikan bahwa dokumen rencanany a menyatakan bahwa sponsor rencana akan secara wajar dan tepat melindung i informasi kesehatan yang dilindung i elektronik yang dibuat, diterima, dipelihara, atau dikirimkan ke atau oleh sponsor rencana atas nama rencana kesehatan kelompok.	rds-snapshot-encry pted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (1)	(b) (1) Standar: Persyaratan untuk rencana kesehatan kelompok. Kecuali jika satu-satunya informasi kesehatan yang dilindungi secara elektronik yang diungkapkan kepada sponsor rencana diungkapkan sesuai dengan ¤164.504 (f) (1) (ii) atau (iii), atau sebagaimana diizinkan berdasark an ¤164.508, rencana kesehatan kelompok harus memastikan bahwa dokumen rencanany a menyatakan bahwa sponsor rencana akan secara wajar dan tepat melindung i informasi kesehatan yang dilindung i elektronik yang dibuat, diterima, dipelihara, atau dikirimkan ke atau oleh sponsor rencana atas nama rencana kesehatan kelompok.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (1)	(b) (1) Standar: Persyaratan untuk rencana kesehatan kelompok. Kecuali jika satu-satunya informasi kesehatan yang dilindungi secara elektronik yang diungkapkan kepada sponsor rencana diungkapkan sesuai dengan ¤164.504 (f) (1) (ii) atau (iii), atau sebagaimana diizinkan berdasark an ¤164.508, rencana kesehatan kelompok harus memastikan bahwa dokumen rencanany a menyatakan bahwa sponsor rencana akan secara wajar dan tepat melindung i informasi kesehatan yang dilindung i elektronik yang dibuat, diterima, dipelihara, atau dikirimkan ke atau oleh sponsor rencana atas nama rencana kesehatan kelompok.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (1)	(b) (1) Standar: Persyaratan untuk rencana kesehatan kelompok. Kecuali jika satu-satunya informasi kesehatan yang dilindungi secara elektronik yang diungkapkan kepada sponsor rencana diungkapkan sesuai dengan ¤164.504 (f) (1) (ii) atau (iii), atau sebagaimana diizinkan berdasark an ¤164.508, rencana kesehatan kelompok harus memastikan bahwa dokumen rencanany a menyatakan bahwa sponsor rencana akan secara wajar dan tepat melindung i informasi kesehatan yang dilindung i elektronik yang dibuat, diterima, dipelihara, atau dikirimkan ke atau oleh sponsor rencana atas nama rencana kesehatan kelompok.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (1)	(b) (1) Standar: Persyaratan untuk rencana kesehatan kelompok. Kecuali jika satu-satunya informasi kesehatan yang dilindungi secara elektronik yang diungkapkan kepada sponsor rencana diungkapkan sesuai dengan ¤164.504 (f) (1) (ii) atau (iii), atau sebagaimana diizinkan berdasark an ¤164.508, rencana kesehatan kelompok harus memastikan bahwa dokumen rencanany a menyatakan bahwa sponsor rencana akan secara wajar dan tepat melindung i informasi kesehatan yang dilindung i elektronik yang dibuat, diterima, dipelihara, atau dikirimkan ke atau oleh sponsor rencana atas nama rencana kesehatan kelompok.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (1)	(b) (1) Standar: Persyaratan untuk rencana kesehatan kelompok. Kecuali jika satu-satunya informasi kesehatan yang dilindungi secara elektronik yang diungkapkan kepada sponsor rencana diungkapkan sesuai dengan ¤164.504 (f) (1) (ii) atau (iii), atau sebagaimana diizinkan berdasark an ¤164.508, rencana kesehatan kelompok harus memastikan bahwa dokumen rencanany a menyatakan bahwa sponsor rencana akan secara wajar dan tepat melindung i informasi kesehatan yang dilindung i elektronik yang dibuat, diterima, dipelihara, atau dikirimkan ke atau oleh sponsor rencana atas nama rencana kesehatan kelompok.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (1)	(b) (1) Standar: Persyaratan untuk rencana kesehatan kelompok. Kecuali jika satu-satunya informasi kesehatan yang dilindungi secara elektronik yang diungkapkan kepada sponsor rencana diungkapkan sesuai dengan ¤164.504 (f) (1) (ii) atau (iii), atau sebagaimana diizinkan berdasark an ¤164.508, rencana kesehatan kelompok harus memastikan bahwa dokumen rencanany a menyatakan bahwa sponsor rencana akan secara wajar dan tepat melindung i informasi kesehatan yang dilindung i elektronik yang dibuat, diterima, dipelihara, atau dikirimkan ke atau oleh sponsor rencana atas nama rencana kesehatan kelompok.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (1)	(b) (1) Standar: Persyaratan untuk rencana kesehatan kelompok. Kecuali jika satu-satunya informasi kesehatan yang dilindungi secara elektronik yang diungkapkan kepada sponsor rencana diungkapkan sesuai dengan ¤164.504 (f) (1) (ii) atau (iii), atau sebagaimana diizinkan berdasark an ¤164.508, rencana kesehatan kelompok harus memastikan bahwa dokumen rencanany a menyatakan bahwa sponsor rencana akan secara wajar dan tepat melindung i informasi kesehatan yang dilindung i elektronik yang dibuat, diterima, dipelihara, atau dikirimkan ke atau oleh sponsor rencana atas nama rencana kesehatan kelompok.	s3- bucket-ssl-request s-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (1)	(b) (1) Standar: Persyaratan untuk rencana kesehatan kelompok. Kecuali jika satu-satunya informasi kesehatan yang dilindungi secara elektronik yang diungkapkan kepada sponsor rencana diungkapkan sesuai dengan ¤164.504 (f) (1) (ii) atau (iii), atau sebagaimana diizinkan berdasark an ¤164.508, rencana kesehatan kelompok harus memastikan bahwa dokumen rencanany a menyatakan bahwa sponsor rencana akan secara wajar dan tepat melindung i informasi kesehatan yang dilindung i elektronik yang dibuat, diterima, dipelihara, atau dikirimkan ke atau oleh sponsor rencana atas nama rencana kesehatan kelompok.	s3- default-encryption -kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (1)	(b) (1) Standar: Persyaratan untuk rencana kesehatan kelompok. Kecuali jika satu-satunya informasi kesehatan yang dilindungi secara elektronik yang diungkapkan kepada sponsor rencana diungkapkan sesuai dengan ¤164.504 (f) (1) (ii) atau (iii), atau sebagaimana diizinkan berdasark an ¤164.508, rencana kesehatan kelompok harus memastikan bahwa dokumen rencanany a menyatakan bahwa sponsor rencana akan secara wajar dan tepat melindung i informasi kesehatan yang dilindung i elektronik yang dibuat, diterima, dipelihara, atau dikirimkan ke atau oleh sponsor rencana atas nama rencana kesehatan kelompok.	sagemaker-endpoint -configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (1)	(b) (1) Standar: Persyaratan untuk rencana kesehatan kelompok. Kecuali jika satu-satunya informasi kesehatan yang dilindungi secara elektronik yang diungkapkan kepada sponsor rencana diungkapkan sesuai dengan ¤164.504 (f) (1) (ii) atau (iii), atau sebagaimana diizinkan berdasark an ¤164.508, rencana kesehatan kelompok harus memastikan bahwa dokumen rencanany a menyatakan bahwa sponsor rencana akan secara wajar dan tepat melindung i informasi kesehatan yang dilindung i elektronik yang dibuat, diterima, dipelihara, atau dikirimkan ke atau oleh sponsor rencana atas nama rencana kesehatan kelompok.	sagemaker-notebook -instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok; (ii) Memastikan bahwa pemisahan yang memadai diperlukan oleh ¤164.504 (f (2) (iii) didukung oleh langkah-langkah keamanan yang	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrai l jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	wajar dan tepat; (iii) Memastikan bahwa agen, termasuk subkontraktor, kepada siapa ia memberika n informasi ini setuju untuk menerapka n langkah-langkah keamanan yang wajar dan tepat untuk melindungi informasi; dan (iv) Melaporkan kepada rencana kesehatan kelompok setiap insiden keamanan yang menjadi sadar.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok; (ii) Memastikan bahwa pemisahan yang memadai diperlukan oleh ¤164.504 (f (2) (iii) didukung oleh langkah-langkah keamanan yang	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	wajar dan tepat; (iii) Memastikan bahwa agen, termasuk subkontraktor, kepada siapa ia memberika n informasi ini setuju untuk menerapka n langkah-langkah keamanan yang wajar dan tepat untuk melindungi informasi; dan (iv) Melaporkan kepada rencana kesehatan kelompok setiap insiden keamanan yang menjadi sadar.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksanakan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integritas, dan ketersediaan informasi kesehatan yang dilindungi elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok; (ii) Memastikan bahwa pemisahan yang memadai diperlukan oleh ¤164.504 (f (2) (iii) didukung oleh langkah-langkah keamanan yang	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	wajar dan tepat; (iii) Memastikan bahwa agen, termasuk subkontraktor, kepada siapa ia memberika n informasi ini setuju untuk menerapka n langkah-langkah keamanan yang wajar dan tepat untuk melindungi informasi; dan (iv) Melaporkan kepada rencana kesehatan kelompok setiap insiden keamanan yang menjadi sadar.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok; (ii) Memastikan bahwa pemisahan yang memadai diperlukan oleh ¤164.504 (f (2) (iii) didukung oleh langkah-langkah keamanan yang	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-n ode enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkrip si memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	wajar dan tepat; (iii) Memastikan bahwa agen, termasuk subkontraktor, kepada siapa ia memberika n informasi ini setuju untuk menerapka n langkah-langkah keamanan yang wajar dan tepat untuk melindungi informasi; dan (iv) Melaporkan kepada rencana kesehatan kelompok setiap insiden keamanan yang menjadi sadar.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok; (ii) Memastikan bahwa pemisahan yang memadai diperlukan oleh ¤164.504 (f (2) (iii) didukung oleh langkah-langkah keamanan yang	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	wajar dan tepat; (iii) Memastikan bahwa agen, termasuk subkontraktor, kepada siapa ia memberika n informasi ini setuju untuk menerapka n langkah-langkah keamanan yang wajar dan tepat untuk melindungi informasi; dan (iv) Melaporkan kepada rencana kesehatan kelompok setiap insiden keamanan yang menjadi sadar.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok; (ii) Memastikan bahwa pemisahan yang memadai diperlukan oleh ¤164.504 (f (2) (iii) didukung oleh langkah-langkah keamanan yang	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	wajar dan tepat; (iii) Memastikan bahwa agen, termasuk subkontraktor, kepada siapa ia memberika n informasi ini setuju untuk menerapka n langkah-langkah keamanan yang wajar dan tepat untuk melindungi informasi; dan (iv) Melaporkan kepada rencana kesehatan kelompok setiap insiden keamanan yang menjadi sadar.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok; (ii) Memastikan bahwa pemisahan yang memadai diperlukan oleh ¤164.504 (f (2) (iii) didukung oleh langkah-langkah keamanan yang	opensearch-encrypt ed-at-rest	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk domain OpenSearc h Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	wajar dan tepat; (iii) Memastikan bahwa agen, termasuk subkontraktor, kepada siapa ia memberika n informasi ini setuju untuk menerapka n langkah-langkah keamanan yang wajar dan tepat untuk melindungi informasi; dan (iv) Melaporkan kepada rencana kesehatan kelompok setiap insiden keamanan yang menjadi sadar.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok; (ii) Memastikan bahwa pemisahan yang memadai diperlukan oleh ¤164.504 (f (2) (iii) didukung oleh langkah-langkah keamanan yang	opensearch-https-r equired	Karena data sensitif dapat ada dan membantu melindung i data dalam perjalana n, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	wajar dan tepat; (iii) Memastikan bahwa agen, termasuk subkontraktor, kepada siapa ia memberika n informasi ini setuju untuk menerapka n langkah-langkah keamanan yang wajar dan tepat untuk melindungi informasi; dan (iv) Melaporkan kepada rencana kesehatan kelompok setiap insiden keamanan yang menjadi sadar.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksanakan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integritas, dan ketersediaan informasi kesehatan yang dilindungi elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok; (ii) Memastikan bahwa pemisahan yang memadai diperlukan oleh ¤164.504 (f (2) (iii) didukung oleh langkah-langkah keamanan yang	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	wajar dan tepat; (iii) Memastikan bahwa agen, termasuk subkontraktor, kepada siapa ia memberika n informasi ini setuju untuk menerapka n langkah-langkah keamanan yang wajar dan tepat untuk melindungi informasi; dan (iv) Melaporkan kepada rencana kesehatan kelompok setiap insiden keamanan yang menjadi sadar.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok; (ii) Memastikan bahwa pemisahan yang memadai diperlukan oleh ¤164.504 (f (2) (iii) didukung oleh langkah-langkah keamanan yang	rds-snapshot-encry pted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	wajar dan tepat; (iii) Memastikan bahwa agen, termasuk subkontraktor, kepada siapa ia memberika n informasi ini setuju untuk menerapka n langkah-langkah keamanan yang wajar dan tepat untuk melindungi informasi; dan (iv) Melaporkan kepada rencana kesehatan kelompok setiap insiden keamanan yang menjadi sadar.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok; (ii) Memastikan bahwa pemisahan yang memadai diperlukan oleh ¤164.504 (f (2) (iii) didukung oleh langkah-langkah keamanan yang	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	wajar dan tepat; (iii) Memastikan bahwa agen, termasuk subkontraktor, kepada siapa ia memberika n informasi ini setuju untuk menerapka n langkah-langkah keamanan yang wajar dan tepat untuk melindungi informasi; dan (iv) Melaporkan kepada rencana kesehatan kelompok setiap insiden keamanan yang menjadi sadar.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok; (ii) Memastikan bahwa pemisahan yang memadai diperlukan oleh ¤164.504 (f (2) (iii) didukung oleh langkah-langkah keamanan yang	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	wajar dan tepat; (iii) Memastikan bahwa agen, termasuk subkontraktor, kepada siapa ia memberika n informasi ini setuju untuk menerapka n langkah-langkah keamanan yang wajar dan tepat untuk melindungi informasi; dan (iv) Melaporkan kepada rencana kesehatan kelompok setiap insiden keamanan yang menjadi sadar.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok; (ii) Memastikan bahwa pemisahan yang memadai diperlukan oleh ¤164.504 (f (2) (iii) didukung oleh langkah-langkah keamanan yang	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	wajar dan tepat; (iii) Memastikan bahwa agen, termasuk subkontraktor, kepada siapa ia memberika n informasi ini setuju untuk menerapka n langkah-langkah keamanan yang wajar dan tepat untuk melindungi informasi; dan (iv) Melaporkan kepada rencana kesehatan kelompok setiap insiden keamanan yang menjadi sadar.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok; (ii) Memastikan bahwa pemisahan yang memadai diperlukan oleh ¤164.504 (f (2) (iii) didukung oleh langkah-langkah keamanan yang	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	wajar dan tepat; (iii) Memastikan bahwa agen, termasuk subkontraktor, kepada siapa ia memberika n informasi ini setuju untuk menerapka n langkah-langkah keamanan yang wajar dan tepat untuk melindungi informasi; dan (iv) Melaporkan kepada rencana kesehatan kelompok setiap insiden keamanan yang menjadi sadar.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok; (ii) Memastikan bahwa pemisahan yang memadai diperlukan oleh ¤164.504 (f (2) (iii) didukung oleh langkah-langkah keamanan yang	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	wajar dan tepat; (iii) Memastikan bahwa agen, termasuk subkontraktor, kepada siapa ia memberika n informasi ini setuju untuk menerapka n langkah-langkah keamanan yang wajar dan tepat untuk melindungi informasi; dan (iv) Melaporkan kepada rencana kesehatan kelompok setiap insiden keamanan yang menjadi sadar.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok; (ii) Memastikan bahwa pemisahan yang memadai diperlukan oleh ¤164.504 (f (2) (iii) didukung oleh langkah-langkah keamanan yang	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	wajar dan tepat; (iii) Memastikan bahwa agen, termasuk subkontraktor, kepada siapa ia memberika n informasi ini setuju untuk menerapka n langkah-langkah keamanan yang wajar dan tepat untuk melindungi informasi; dan (iv) Melaporkan kepada rencana kesehatan kelompok setiap insiden keamanan yang menjadi sadar.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok; (ii) Memastikan bahwa pemisahan yang memadai diperlukan oleh ¤164.504 (f (2) (iii) didukung oleh langkah-langkah keamanan yang	s3- bucket-ssl-request s-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	wajar dan tepat; (iii) Memastikan bahwa agen, termasuk subkontraktor, kepada siapa ia memberika n informasi ini setuju untuk menerapka n langkah-langkah keamanan yang wajar dan tepat untuk melindungi informasi; dan (iv) Melaporkan kepada rencana kesehatan kelompok setiap insiden keamanan yang menjadi sadar.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok; (ii) Memastikan bahwa pemisahan yang memadai diperlukan oleh ¤164.504 (f (2) (iii) didukung oleh langkah-langkah keamanan yang	s3- default-encryption -kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	wajar dan tepat; (iii) Memastikan bahwa agen, termasuk subkontraktor, kepada siapa ia memberika n informasi ini setuju untuk menerapka n langkah-langkah keamanan yang wajar dan tepat untuk melindungi informasi; dan (iv) Melaporkan kepada rencana kesehatan kelompok setiap insiden keamanan yang menjadi sadar.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok; (ii) Memastikan bahwa pemisahan yang memadai diperlukan oleh ¤164.504 (f (2) (iii) didukung oleh langkah-langkah keamanan yang	sagemaker-endpoint -configuration-kms- kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	wajar dan tepat; (iii) Memastikan bahwa agen, termasuk subkontraktor, kepada siapa ia memberika n informasi ini setuju untuk menerapka n langkah-langkah keamanan yang wajar dan tepat untuk melindungi informasi; dan (iv) Melaporkan kepada rencana kesehatan kelompok setiap insiden keamanan yang menjadi sadar.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok; (ii) Memastikan bahwa pemisahan yang memadai diperlukan oleh ¤164.504 (f (2) (iii) didukung oleh langkah-langkah keamanan yang	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	wajar dan tepat; (iii) Memastikan bahwa agen, termasuk subkontraktor, kepada siapa ia memberika n informasi ini setuju untuk menerapka n langkah-langkah keamanan yang wajar dan tepat untuk melindungi informasi; dan (iv) Melaporkan kepada rencana kesehatan kelompok setiap insiden keamanan yang menjadi sadar.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	iam-user-no-policies-periksa	Aturan ini memastika n kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapka n hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	iam-policy-no-stat ements-with-full-a ccess	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	ecs-containers-rea donly-access	Mengaktifkan akses baca saja ke wadah Amazon Elastic Container Service (ECS) dapat membantu mematuhi prinsip hak istimewa yang paling rendah. Opsi ini dapat mengurangi vektor serangan karena sistem file instance container tidak dapat dimodifikasi kecuali jika memiliki izin baca-tulis eksplisit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	s3- bucket-acl-prohibi ted	Aturan ini memeriksa untuk melihat apakah Daftar Kontrol Akses (ACLs) digunakan untuk kontrol akses di Bucket Amazon S3. ACLs adalah mekanisme kontrol akses lama untuk bucket Amazon S3 yang AWS mendahulu i Identity and Access Management (IAM). Sebagai gantinya ACLs, ini adalah praktik terbaik untuk menggunakan kebijakan IAM atau kebijakan bucket S3 untuk mengelola akses ke bucket S3 Anda dengan lebih mudah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifik asi berdasark an kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkin kan Anda untuk mengatur secara opsional RequireUp percaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	acm-certificate-ex piration-check	Pastikan integritas jaringan dilindungi dengan memastika n sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExp iration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	elb-predefined-sec urity-policy-ssl-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa pendengar SSL Classic Elastic Load Balancing Anda menggunakan kebijakan keamanan yang telah ditentuka n sebelumnya. Elastic Load Balancing menyediakan konfigurasi negosiasi SSL yang telah ditentukan sebelumny a yang digunakan untuk negosiasi SSL ketika koneksi dibuat antara klien dan penyeimba ng beban Anda. Konfigurasi negosiasi SSL memberika n kompatibilitas dengan berbagai klien dan menggunakan algoritma kriptogra fi berkekuatan tinggi. Aturan ini mengharuskan Anda menetapkan kebijakan keamanan yang telah ditentuka

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			n untuk pendengar SSL Anda. Kebijakan keamanan default adalah: ELBSecurity Policy-TLS-1-2-2017-0. Nilai aktual harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	s3- bucket-ssl-request s-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrai l jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksanakan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integritas, dan ketersediaan informasi kesehatan yang dilindungi elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-n ode enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkrip si memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	rds-snapshot-encry pted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksanakan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integritas, dan ketersediaan informasi kesehatan yang dilindungi elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	s3- default-encryption -kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	sagemaker-endpoint -configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	dynamodb-autoscali ng-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughpu t yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tuli s yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	dynamodb-pitr-enab led	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertah ankan cadangan dengan memastika n bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	elb-cross-zone-loa d-menyeimbangkan diaktifkan	Aktifkan penyeimba ngan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimba ngan beban lintas zona mengurang i kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkat kan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	elb-deletion-prote ction-enabled	Aturan ini memastika n bahwa Elastic Load Balancing memiliki perlindun gan penghapus an yang diaktifka n. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersedi aan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	rds-cluster-deletion-protection-diaktifkan	Pastikan instans Amazon Relationa l Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindun gan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersedi aan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) menyediakan ketersediaan dan daya tahan yang ditingkatkan untuk instans database. Saat Anda menyediak an instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastru ktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutk an operasi database

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			segera setelah failover selesai.
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	s3- bucket-default-loc k-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimpleme ntasikan untuk mencapai persyarat an ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivi tas jika salah satu koneksi Site-to-S ite VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivi tas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksanakan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integritas, dan ketersediaan informasi kesehatan yang dilindungi elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	opensearch-https-r equired	Karena data sensitif dapat ada dan membantu melindung i data dalam perjalana n, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	opensearch-node-to -node-pemeriksaan enkripsi-	Pastikan node-to-n ode enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkrip si memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
164.314 (b) (2) (i)	(2) Spesifikasi implementasi (Wajib). Dokumen rencana rencana kesehatan kelompok harus diubah untuk memasukkan ketentuan untuk mewajibkan sponsor rencana untuk - (i) Melaksana kan pengamanan administratif, fisik, dan teknis yang secara wajar dan tepat melindungi kerahasiaan, integrita s, dan ketersediaan informasi kesehatan yang dilindung i elektronik yang dibuat, menerima, memelihara, atau mentransmisikan atas nama rencana kesehatan kelompok;	kinesis-stream-enc rypted	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Keamanan HIPAA.

Praktik Terbaik Operasional untuk IRS 1075

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan

biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara IRS 1075 dan aturan AWS Config terkelola. Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan berhubungan dengan satu atau lebih kontrol IRS 1075. Kontrol IRS 1075 dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1 Komputasi Awan d. Enkripsi Data dalam Transit	FTI harus dienkrips i dalam perjalana n dalam lingkunga n cloud. Semua mekanisme yang digunakan untuk mengenkripsi FTI harus bersertif ikat FIPS 140 dan beroperas i menggunakan modul FIPS 140 terbaru yang sesuai. Persyaratan ini harus dimasukkan dalam SLA.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
3.3.1 Komputasi Awan d. Enkripsi Data dalam Transit	FTI harus dienkrips i dalam perjalana n dalam lingkunga n cloud. Semua mekanisme yang digunakan untuk mengenkripsi FTI	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-n ode enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkrip si memungkinkan enkripsi TLS 1.2 untuk

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	harus bersertif ikat FIPS 140 dan beroperas i menggunakan modul FIPS 140 terbaru yang sesuai. Persyaratan ini harus dimasukkan dalam SLA.		semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
3.3.1 Komputasi Awan d. Enkripsi Data dalam Transit	FTI harus dienkrips i dalam perjalana n dalam lingkunga n cloud. Semua mekanisme yang digunakan untuk mengenkripsi FTI harus bersertif ikat FIPS 140 dan beroperas i menggunakan modul FIPS 140 terbaru yang sesuai. Persyaratan ini harus dimasukkan dalam SLA.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1 Komputasi Awan d. Enkripsi Data dalam Transit	FTI harus dienkrips i dalam perjalana n dalam lingkunga n cloud. Semua mekanisme yang digunakan untuk mengenkripsi FTI harus bersertif ikat FIPS 140 dan beroperas i menggunakan modul FIPS 140 terbaru yang sesuai. Persyaratan ini harus dimasukkan dalam SLA.	opensearch-https-r equired	Karena data sensitif dapat ada dan membantu melindung i data dalam perjalana n, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
3.3.1 Komputasi Awan d. Enkripsi Data dalam Transit	FTI harus dienkrips i dalam perjalana n dalam lingkunga n cloud. Semua mekanisme yang digunakan untuk mengenkripsi FTI harus bersertif ikat FIPS 140 dan beroperas i menggunakan modul FIPS 140 terbaru yang sesuai. Persyaratan ini harus dimasukkan dalam SLA.	opensearch-node-to -node-pemeriksaan enkripsi-	Pastikan node-to-n ode enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkrip si memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1 Komputasi Awan d. Enkripsi Data dalam Transit	FTI harus dienkrips i dalam perjalana n dalam lingkunga n cloud. Semua mekanisme yang digunakan untuk mengenkripsi FTI harus bersertif ikat FIPS 140 dan beroperas i menggunakan modul FIPS 140 terbaru yang sesuai. Persyaratan ini harus dimasukkan dalam SLA.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
3.3.1 Komputasi Awan d. Enkripsi Data dalam Transit	FTI harus dienkrips i dalam perjalana n dalam lingkunga n cloud. Semua mekanisme yang digunakan untuk mengenkripsi FTI harus bersertif ikat FIPS 140 dan beroperas i menggunakan modul FIPS 140 terbaru yang sesuai. Persyaratan ini harus dimasukkan dalam SLA.	s3- bucket-ssl-request s-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1 Komputasi Awan e. Enkripsi Data saat Istirahat	Enkripsi Data saat Istirahat: FTI harus dienkripsi saat diam di cloud menggunakan mekanisme enkripsi bersertifikat FIPS 140 terbaru. Persyaratan ini harus dimasukkan dalam SLA.	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
3.3.1 Komputasi Awan e. Enkripsi Data saat Istirahat	Enkripsi Data saat Istirahat: FTI harus dienkripsi saat diam di cloud menggunakan mekanisme enkripsi bersertifikat FIPS 140 terbaru. Persyaratan ini harus dimasukkan dalam SLA.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
3.3.1 Komputasi Awan e. Enkripsi Data saat Istirahat	Enkripsi Data saat Istirahat: FTI harus dienkripsi saat diam di cloud menggunakan mekanisme enkripsi bersertifikat FIPS 140 terbaru. Persyaratan ini harus dimasukkan dalam SLA.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1 Komputasi Awan e. Enkripsi Data saat Istirahat	Enkripsi Data saat Istirahat: FTI harus dienkripsi saat diam di cloud menggunakan mekanisme enkripsi bersertifikat FIPS 140 terbaru. Persyaratan ini harus dimasukkan dalam SLA.	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
3.3.1 Komputasi Awan e. Enkripsi Data saat Istirahat	Enkripsi Data saat Istirahat: FTI harus dienkripsi saat diam di cloud menggunakan mekanisme enkripsi bersertifikat FIPS 140 terbaru. Persyaratan ini harus dimasukkan dalam SLA.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1 Komputasi Awan e. Enkripsi Data saat Istirahat	Enkripsi Data saat Istirahat: FTI harus dienkripsi saat diam di cloud menggunakan mekanisme enkripsi bersertifikat FIPS 140 terbaru. Persyaratan ini harus dimasukkan dalam SLA.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
3.3.1 Komputasi Awan e. Enkripsi Data saat Istirahat	Enkripsi Data saat Istirahat: FTI harus dienkripsi saat diam di cloud menggunakan mekanisme enkripsi bersertifikat FIPS 140 terbaru. Persyaratan ini harus dimasukkan dalam SLA.	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
3.3.1 Komputasi Awan e. Enkripsi Data saat Istirahat	Enkripsi Data saat Istirahat: FTI harus dienkripsi saat diam di cloud menggunakan mekanisme enkripsi bersertifikat FIPS 140 terbaru. Persyaratan ini harus dimasukkan dalam SLA.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1 Komputasi Awan e. Enkripsi Data saat Istirahat	Enkripsi Data saat Istirahat: FTI harus dienkripsi saat diam di cloud menggunakan mekanisme enkripsi bersertifikat FIPS 140 terbaru. Persyaratan ini harus dimasukkan dalam SLA.	kinesis-stream-encrypted	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.
3.3.1 Komputasi Awan e. Enkripsi Data saat Istirahat	Enkripsi Data saat Istirahat: FTI harus dienkripsi saat diam di cloud menggunakan mekanisme enkripsi bersertifikat FIPS 140 terbaru. Persyaratan ini harus dimasukkan dalam SLA.	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
3.3.1 Komputasi Awan e. Enkripsi Data saat Istirahat	Enkripsi Data saat Istirahat: FTI harus dienkripsi saat diam di cloud menggunakan mekanisme enkripsi bersertifikat FIPS 140 terbaru. Persyaratan ini harus dimasukkan dalam SLA.	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1 Komputasi Awan e. Enkripsi Data saat Istirahat	Enkripsi Data saat Istirahat: FTI harus dienkripsi saat diam di cloud menggunakan mekanisme enkripsi bersertifikat FIPS 140 terbaru. Persyaratan ini harus dimasukkan dalam SLA.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1 Komputasi Awan e. Enkripsi Data saat Istirahat	Enkripsi Data saat Istirahat: FTI harus dienkripsi saat diam di cloud menggunakan mekanisme enkripsi bersertifikat FIPS 140 terbaru. Persyaratan ini harus dimasukkan dalam SLA.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1 Komputasi Awan e. Enkripsi Data saat Istirahat	Enkripsi Data saat Istirahat: FTI harus dienkripsi saat diam di cloud menggunakan mekanisme enkripsi bersertifikat FIPS 140 terbaru. Persyaratan ini harus dimasukkan dalam SLA.	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
3.3.1 Komputasi Awan e. Enkripsi Data saat Istirahat	Enkripsi Data saat Istirahat: FTI harus dienkripsi saat diam di cloud menggunakan mekanisme enkripsi bersertifikat FIPS 140 terbaru. Persyaratan ini harus dimasukkan dalam SLA.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1 Komputasi Awan e. Enkripsi Data saat Istirahat	Enkripsi Data saat Istirahat: FTI harus dienkripsi saat diam di cloud menggunakan mekanisme enkripsi bersertifikat FIPS 140 terbaru. Persyaratan ini harus dimasukkan dalam SLA.	s3- default-encryption -kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
3.3.1 Komputasi Awan e. Enkripsi Data saat Istirahat	Enkripsi Data saat Istirahat: FTI harus dienkripsi saat diam di cloud menggunakan mekanisme enkripsi bersertifikat FIPS 140 terbaru. Persyaratan ini harus dimasukkan dalam SLA.	sagemaker-endpoint -configuration-kms- kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1 Komputasi Awan e. Enkripsi Data saat Istirahat	Enkripsi Data saat Istirahat: FTI harus dienkripsi saat diam di cloud menggunakan mekanisme enkripsi bersertifikat FIPS 140 terbaru. Persyaratan ini harus dimasukkan dalam SLA.	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
3.3.1 Komputasi Awan e. Enkripsi Data saat Istirahat	Enkripsi Data saat Istirahat: FTI harus dienkripsi saat diam di cloud menggunakan mekanisme enkripsi bersertifikat FIPS 140 terbaru. Persyaratan ini harus dimasukkan dalam SLA.	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1 Komputasi Awan k. Otentikasi Multifaktor	Agensi harus menerapkan otentikasi multifaktor yang memadai ketika solusi cloud mereka tersedia dari internet (yaitu, ada akses ke solusi cloud dari luar jaringan tepercaya agensi).	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1 Komputasi Awan k. Otentikasi Multifaktor	Agensi harus menerapkan otentikasi multifaktor yang memadai ketika solusi cloud mereka tersedia dari internet (yaitu, ada akses ke solusi cloud dari luar jaringan tepercaya agensi).	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1 Komputasi Awan k. Otentikasi Multifaktor	Agensi harus menerapkan otentikasi multifaktor yang memadai ketika solusi cloud mereka tersedia dari internet (yaitu, ada akses ke solusi cloud dari luar jaringan tepercaya agensi).	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1 Komputasi Awan k. Otentikasi Multifaktor	Agensi harus menerapkan otentikasi multifaktor yang memadai ketika solusi cloud mereka tersedia dari internet (yaitu, ada akses ke solusi cloud dari luar jaringan tepercaya agensi).	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1 Komputasi Awan i. Penilaian Risiko:	Agensi harus melakukan penilaian tahunan terhadap kontrol keamanan dan privasi yang berlaku pada semua sistem informasi yang digunakan untuk menerima, memproses , menyimpan , mengakses, melindungi dan/atau mentransmisikan FTI.	annual-risk-assessment-performed(Pemeriksaan Proses)	Lakukan penilaian risiko tahunan pada organisasi Anda. Penilaian risiko dapat membantu dalam menentukan kemungkinan dan dampak dari risiko dan/atau kerentanan yang diidentifikasi yang mempengaruhi suatu organisasi.
3.3.6 Batas Jaringan dan Infrastruktur	Agensi harus menerapkan perangkat perlindungan batas di seluruh arsitektur sistem mereka, termasuk router, firewall, switch, dan sistem deteksi intrusi untuk melindungi sistem FTI dan FTI.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.6 Batas Jaringan dan Infrastruktur	Agensi harus menerapkan perangkat perlindungan batas di seluruh arsitektur sistem mereka, termasuk router, firewall, switch, dan sistem deteksi intrusi untuk melindungi sistem FTI dan FTI.	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.6 Batas Jaringan dan Infrastruktur	Agensi harus menerapkan perangkat perlindun gan batas di seluruh arsitektur sistem mereka, termasuk router, firewall, switch, dan sistem deteksi intrusi untuk melindungi sistem FTI dan FTI.	netfw-policy-rule-group-terkait	Kebijakan AWS Network Firewall mendefinisikan bagaimana firewall Anda memantau dan menangani lalu lintas di VPC Amazon. Anda mengonfigurasi grup aturan stateless dan stateful untuk memfilter paket dan arus lalu lintas, dan Anda menentuka n penanganan lalu lintas default.
3.3.6 Batas Jaringan dan Infrastruktur	Agensi harus menerapkan perangkat perlindun gan batas di seluruh arsitektur sistem mereka, termasuk router, firewall, switch, dan sistem deteksi intrusi untuk melindungi sistem FTI dan FTI.	netfw-stateless-rule-group-tidak-kosong	Grup aturan AWS Network Firewall berisi aturan yang menentukan bagaimana firewall Anda memproses lalu lintas di VPC Anda. Grup aturan stateless kosong saat ada dalam kebijakan firewall tidak memproses lalu lintas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.6 Batas Jaringan dan Infrastruktur	Agensi harus menerapkan perangkat perlindun gan batas di seluruh arsitektur sistem mereka, termasuk router, firewall, switch, dan sistem deteksi intrusi untuk melindungi sistem FTI dan FTI.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.6 Batas Jaringan dan Infrastruktur	Agensi harus menerapkan perangkat perlindungan batas di seluruh arsitektur sistem mereka, termasuk router, firewall, switch, dan sistem deteksi intrusi untuk melindungi sistem FTI dan FTI.	waf-regional-rule-not-kosong	Pastikan AWS WAF Anda memiliki aturan yang tidak kosong. Aturan tanpa kondisi dapat mengakibatkan perilaku yang tidak diinginkan.
3.3.6 Batas Jaringan dan Infrastruktur	Agensi harus menerapkan perangkat perlindungan batas di seluruh arsitektur sistem mereka, termasuk router, firewall, switch, dan sistem deteksi intrusi untuk melindungi sistem FTI dan FTI.	waf-regional-rulegroup-not-kosong	Pastikan AWS WAF Anda memiliki grup aturan yang tidak kosong. Grup aturan yang kosong dapat mengakibatkan perilaku yang tidak diinginkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.6 Batas Jaringan dan Infrastruktur	Agensi harus menerapkan perangkat perlindun gan batas di seluruh arsitektur sistem mereka, termasuk router, firewall, switch, dan sistem deteksi intrusi untuk melindungi sistem FTI dan FTI.	waf-regional-webacl-not-kosong	Web ACL yang dilampirkan ke AWS WAF dapat berisi kumpulan aturan dan kelompok aturan untuk memeriksa dan mengontrol permintaan web. Jika ACL Web kosong, lalu lintas web lewat tanpa terdeteksi atau ditindaklanjuti oleh WAF.
3.3.6 Batas Jaringan dan Infrastruktur	Agensi harus menerapkan perangkat perlindun gan batas di seluruh arsitektur sistem mereka, termasuk router, firewall, switch, dan sistem deteksi intrusi untuk melindungi sistem FTI dan FTI.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.6 Batas Jaringan dan Infrastruktur	Agensi harus menerapkan perangkat perlindun gan batas di seluruh arsitektur sistem mereka, termasuk router, firewall, switch, dan sistem deteksi intrusi untuk melindungi sistem FTI dan FTI.	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizink an, memblokir, atau menghitung permintaa n web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindung inya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 Manajemen Akun (f)	Membuat, mengaktifkan, memodifikasi, menonaktifkan, dan menghapus akun sesuai dengan prasyarat prosedur manajemen akun agensi;	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 Manajemen Akun (f)	Membuat, mengaktif kan, memodifikasi, menonaktifkan, dan menghapus akun sesuai dengan prasyarat prosedur manajemen akun agensi;	account-part-of-or ganizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastika n bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.
AC-2 Manajemen Akun (f)	Membuat, mengaktif kan, memodifikasi, menonaktifkan, dan menghapus akun sesuai dengan prasyarat prosedur manajemen akun agensi;	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 Manajemen Akun (f)	Membuat, mengaktif kan, memodifikasi, menonaktifkan, dan menghapus akun sesuai dengan prasyarat prosedur manajemen akun agensi;	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastika n otentikasi multi-fak tor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 Manajemen Akun (f)	Membuat, mengaktif kan, memodifikasi, menonaktifkan, dan menghapus akun sesuai dengan prasyarat prosedur manajemen akun agensi;	iam-user-no-policies-periksa	Aturan ini memastika n kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapka n hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 Manajemen Akun (g)	Pantau penggunaan akun	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
AC-2 Manajemen Akun (g)	Pantau penggunaan akun	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 Manajemen Akun (g)	Pantau penggunaan akun	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 Manajemen Akun (g)	Pantau penggunaan akun	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 Manajemen Akun (g)	Pantau penggunaan akun	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 Manajemen Akun (g)	Pantau penggunaan akun	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 Manajemen Akun (g)	Pantau penggunaan akun	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 Manajemen Akun (g)	Pantau penggunaan akun	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 Manajemen Akun (j)	Tinjau akun untuk kepatuhan dengan persyaratan manajemen akun	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 Manajemen Akun (j)	Tinjau akun untuk kepatuhan dengan persyaratan manajemen akun	secretsmanager-scheduled-rotation-success-periksa	Aturan ini memastikan bahwa AWS rahasia Secrets Manager telah berhasil diputar sesuai dengan jadwal rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode di mana rahasia aktif, dan berpotensi mengurangi dampak bisnis jika dikompromikan.
AC-2 Manajemen Akun (j)	Tinjau akun untuk kepatuhan dengan persyaratan manajemen akun	secretsmanager-secret-periodic-rotation	Aturan ini memastikan AWS rahasia Secrets Manager mengaktifkan rotasi periodik. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan. Nilai defaultnya adalah 90 hari.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 Manajemen Akun (j)	Tinjau akun untuk kepatuhan dengan persyaratan manajemen akun	secretsmanager-secret-unused	Jika kredensyal yang tidak digunakan ada di AWS Secrets Manager, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini memungkinkan Anda untuk menetapkan nilai ke unusedFor Days (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 Manajemen Akun (j)	Tinjau akun untuk kepatuhan dengan persyaratan manajemen akun	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 Manajemen Akun (j)	Tinjau akun untuk kepatuhan dengan persyaratan manajemen akun	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 Manajemen Akun (j)	Tinjau akun untuk kepatuhan dengan persyaratan manajemen akun	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 Manajemen Akun (j)	Tinjau akun untuk kepatuhan dengan persyaratan manajemen akun	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 Manajemen Akun (j)	Tinjau akun untuk kepatuhan dengan persyaratan manajemen akun	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 Manajemen Akun (j)	Tinjau akun untuk kepatuhan dengan persyaratan manajemen akun	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 Manajemen Akun (j)	Tinjau akun untuk kepatuhan dengan persyaratan manajemen akun	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
(CE-1) Manajemen Akun Sistem Otomatis	Mendukung pengelola an akun sistem menggunakan mekanisme otomatis.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifik asi berdasark an kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkin kan Anda untuk mengatur secara opsional RequireUp percaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
(CE-1) Manajemen Akun Sistem Otomatis	Mendukung pengelola an akun sistem menggunakan mekanisme otomatis.	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastika n kunci akses IAM diputar sebagaima na ditentukan oleh kebijakan organisas i. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurang i dampak bisnis jika kunci dikompromikan. Aturan ini memerluka n nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
(CE-1) Manajemen Akun Sistem Otomatis	Mendukung pengelola an akun sistem menggunakan mekanisme otomatis.	secretsmanager-sch eduled-rotation-su ccess-periksa	Aturan ini memastika n bahwa AWS rahasia Secrets Manager telah berhasil diputar sesuai dengan jadwal rotasi. Memutar rahasia pada jadwal reguler dapat mempersin gkat periode di mana rahasia aktif, dan berpotensi mengurangi dampak bisnis jika dikomprom ikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
(CE-3): Nonaktifkan Akun	Nonaktifkan akun dalam 120 hari ketika akun: a. Telah kedaluwarsa; b. Tidak lagi terkait dengan pengguna atau individu; c. Melanggar kebijakan organisasi; atau d. Tidak aktif selama 120 hari untuk akun yang tidak memiliki hak istimewa dan 60 hari untuk akun istimewa	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
(CE-12) Pemantauan Akun untuk Penggunaan Atipikal	Memantau akun sistem untuk penggunaan atipikal yang ditentukan oleh agensi; dan Laporkan penggunaan akun sistem yang tidak lazim kepada personel atau peran yang ditentukan lembaga.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Hak Istimewa Terkecil AC-6	Menggunakan prinsip hak istimewa terkecil, hanya mengizinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas organisasi yang ditugaskan.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
Hak Istimewa Terkecil AC-6	Menggunakan prinsip hak istimewa terkecil, hanya mengizinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas organisasi yang ditugaskan.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Hak Istimewa Terkecil AC-6	Menggunakan prinsip hak istimewa terkecil, hanya mengizinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas organisasi yang ditugaskan.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Hak Istimewa Terkecil AC-6	Menggunakan prinsip hak istimewa terkecil, hanya mengizinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas organisasi yang ditugaskan.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Hak Istimewa Terkecil AC-6	Menggunakan prinsip hak istimewa terkecil, hanya mengizinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas organisasi yang ditugaskan.	opensearch-access-control-enabled	Pastikan kontrol akses berbutir halus diaktifkan di domain Layanan Amazon OpenSearch Anda. Kontrol akses berbutir halus menyediakan mekanisme otorisasi yang disempurnakan untuk mencapai akses yang paling tidak memiliki hak istimewa ke domain Layanan Amazon. OpenSearch Ini memungkinkan kontrol akses berbasis peran ke domain, serta indeks, dokumen, dan keamanan tingkat lapangan, dukungan untuk dasbor OpenSearch Layanan multi-tenancy, dan otentikasi dasar HTTP untuk Layanan dan Kibana. OpenSearch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Hak Istimewa Terkecil AC-6	Menggunakan prinsip hak istimewa terkecil, hanya mengizinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas organisasi yang ditugaskan.	secretsmanager-secret-unused	Jika kredensyal yang tidak digunakan ada di AWS Secrets Manager, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini memungkinkan Anda untuk menetapkan nilai ke unusedFor Days (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Hak Istimewa Terkecil AC-6	Menggunakan prinsip hak istimewa terkecil, hanya mengizinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas organisasi yang ditugaskan.	codebuild-project-environment-privileged-periksa	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan lingkungan CodeBuild proyek Amazon Anda tidak mengaktifkan mode istimewa. Pengaturan ini harus dinonaktifkan untuk mencegah akses yang tidak diinginkan ke Docker APIs serta perangkat keras yang mendasarinya.
Hak Istimewa Terkecil AC-6	Menggunakan prinsip hak istimewa terkecil, hanya mengizinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas organisasi yang ditugaskan.	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Hak Istimewa Terkecil AC-6	Menggunakan prinsip hak istimewa terkecil, hanya mengizinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas organisasi yang ditugaskan.	ecs-containers-non privileged	Untuk membantu menerapkan prinsip hak istimewa paling rendah, definisi tugas Amazon Elastic Container Service (Amazon ECS) seharusnya tidak mengaktifkan hak istimewa yang ditinggikan. Ketika parameter ini benar, wadah diberikan hak istimewa yang ditinggikan pada instance wadah host (mirip dengan pengguna root).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Hak Istimewa Terkecil AC-6	Menggunakan prinsip hak istimewa terkecil, hanya mengizinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas organisasi yang ditugaskan.	ecs-containers-readonly-access	Mengaktifkan akses baca saja ke wadah Amazon Elastic Container Service (ECS) dapat membantu mematuhi prinsip hak istimewa yang paling rendah. Opsi ini dapat mengurangi vektor serangan karena sistem file instance container tidak dapat dimodifikasi kecuali jika memiliki izin baca-tulis eksplisit.
Hak Istimewa Terkecil AC-6	Menggunakan prinsip hak istimewa terkecil, hanya mengizinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas organisasi yang ditugaskan.	ecs-task-definition-nonroot-pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan bahwa pengguna non-root ditunjuk untuk mengakses definisi tugas Amazon Elastic Container Service (Amazon ECS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Hak Istimewa Terkecil AC-6	Menggunakan prinsip hak istimewa terkecil, hanya mengizinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas organisasi yang ditugaskan.	efs-access-point-enforce-identitas pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan penegakan pengguna diaktifkan untuk Amazon Elastic File System (Amazon EFS) Anda. Saat diaktifkan, Amazon EFS mengganti kan pengguna dan grup klien NFS IDs dengan identitas yang dikonfigurasi pada titik akses untuk semua operasi sistem file dan hanya memberika n akses ke identitas pengguna yang diberlakukan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Hak Istimewa Terkecil AC-6	Menggunakan prinsip hak istimewa terkecil, hanya mengizinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas organisasi yang ditugaskan.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Hak Istimewa Terkecil AC-6	Menggunakan prinsip hak istimewa terkecil, hanya mengizinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas organisasi yang ditugaskan.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17: Akses Jarak Jauh	Menetapkan dan mendokumentasikan pembatasan penggunaan, persyaratan konfigurasi/koneksi, dan panduan implementasi untuk setiap jenis akses jarak jauh yang diizinkan; dan Otorisasi setiap jenis akses jarak jauh ke sistem sebelum mengizinkan koneksi tersebut.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17: Akses Jarak Jauh	Menetapkan dan mendokumentasikan pembatasan penggunaan, persyaratan konfigurasi/koneksi, dan panduan implementasi untuk setiap jenis akses jarak jauh yang diizinkan; dan Otorisasi setiap jenis akses jarak jauh ke sistem sebelum mengizinkan koneksi tersebut.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17: Akses Jarak Jauh	Menetapkan dan mendokumentasikan pembatasan penggunaan, persyaratan konfigurasi/koneksi, dan panduan implementasi untuk setiap jenis akses jarak jauh yang diizinkan; dan Otorisasi setiap jenis akses jarak jauh ke sistem sebelum mengizinkan koneksi tersebut.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17: Akses Jarak Jauh	Menetapkan dan mendokumentasikan pembatasan penggunaan, persyaratan konfigurasi/koneksi, dan panduan implementasi untuk setiap jenis akses jarak jauh yang diizinkan; dan Otorisasi setiap jenis akses jarak jauh ke sistem sebelum mengizinkan koneksi tersebut.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17: Akses Jarak Jauh	Menetapkan dan mendokumentasikan pembatasan penggunaan, persyaratan konfigurasi/koneksi, dan panduan implementasi untuk setiap jenis akses jarak jauh yang diizinkan; dan Otorisasi setiap jenis akses jarak jauh ke sistem sebelum mengizinkan koneksi tersebut.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17: Akses Jarak Jauh	Menetapkan dan mendokumentasikan pembatasan penggunaan, persyaratan konfigurasi/koneksi, dan panduan implementasi untuk setiap jenis akses jarak jauh yang diizinkan; dan Otorisasi setiap jenis akses jarak jauh ke sistem sebelum mengizinkan koneksi tersebut.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
AC-17: Akses Jarak Jauh	Menetapkan dan mendokumentasikan pembatasan penggunaan, persyaratan konfigurasi/koneksi, dan panduan implementasi untuk setiap jenis akses jarak jauh yang diizinkan; dan Otorisasi setiap jenis akses jarak jauh ke sistem sebelum mengizinkan koneksi tersebut.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17: Akses Jarak Jauh	Menetapkan dan mendokumentasikan pembatasan penggunaan, persyaratan konfigurasi/koneksi, dan panduan implementasi untuk setiap jenis akses jarak jauh yang diizinkan; dan Otorisasi setiap jenis akses jarak jauh ke sistem sebelum mengizinkan koneksi tersebut.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17: Akses Jarak Jauh	Menetapkan dan mendokumentasikan pembatasan penggunaan, persyaratan konfigurasi/koneksi, dan panduan implementasi untuk setiap jenis akses jarak jauh yang diizinkan; dan Otorisasi setiap jenis akses jarak jauh ke sistem sebelum mengizinkan koneksi tersebut.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17: Akses Jarak Jauh	Menetapkan dan mendokumentasikan pembatasan penggunaan, persyaratan konfigurasi/koneksi, dan panduan implementasi untuk setiap jenis akses jarak jauh yang diizinkan; dan Otorisasi setiap jenis akses jarak jauh ke sistem sebelum mengizinkan koneksi tersebut.	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17: Akses Jarak Jauh	Menetapkan dan mendokumentasikan pembatasan penggunaan, persyaratan konfigurasi/koneksi, dan panduan implementasi untuk setiap jenis akses jarak jauh yang diizinkan; dan Otorisasi setiap jenis akses jarak jauh ke sistem sebelum mengizinkan koneksi tersebut.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17: Akses Jarak Jauh	Menetapkan dan mendokumentasikan pembatasan penggunaan, persyaratan konfigurasi/koneksi, dan panduan implementasi untuk setiap jenis akses jarak jauh yang diizinkan; dan Otorisasi setiap jenis akses jarak jauh ke sistem sebelum mengizinkan koneksi tersebut.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17: Akses Jarak Jauh	Menetapkan dan mendokumentasikan pembatasan penggunaan, persyaratan konfigurasi/koneksi, dan panduan implementasi untuk setiap jenis akses jarak jauh yang diizinkan; dan Otorisasi setiap jenis akses jarak jauh ke sistem sebelum mengizinkan koneksi tersebut.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17: Akses Jarak Jauh	Menetapkan dan mendokumentasikan pembatasan penggunaan, persyaratan konfigurasi/koneksi, dan panduan implementasi untuk setiap jenis akses jarak jauh yang diizinkan; dan Otorisasi setiap jenis akses jarak jauh ke sistem sebelum mengizinkan koneksi tersebut.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17: Akses Jarak Jauh	Menetapkan dan mendokumentasikan pembatasan penggunaan, persyaratan konfigurasi/koneksi, dan panduan implementasi untuk setiap jenis akses jarak jauh yang diizinkan; dan Otorisasi setiap jenis akses jarak jauh ke sistem sebelum mengizinkan koneksi tersebut.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17: Akses Jarak Jauh	Menetapkan dan mendokumentasikan pembatasan penggunaan, persyaratan konfigurasi/koneksi, dan panduan implementasi untuk setiap jenis akses jarak jauh yang diizinkan; dan Otorisasi setiap jenis akses jarak jauh ke sistem sebelum mengizinkan koneksi tersebut.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17: Akses Jarak Jauh	Menetapkan dan mendokumentasikan pembatasan penggunaan, persyaratan konfigurasi/koneksi, dan panduan implementasi untuk setiap jenis akses jarak jauh yang diizinkan; dan Otorisasi setiap jenis akses jarak jauh ke sistem sebelum mengizinkan koneksi tersebut.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17: Akses Jarak Jauh	Menetapkan dan mendokumentasikan pembatasan penggunaan, persyaratan konfigurasi/koneksi, dan panduan implementasi untuk setiap jenis akses jarak jauh yang diizinkan; dan Otorisasi setiap jenis akses jarak jauh ke sistem sebelum mengizinkan koneksi tersebut.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17: Akses Jarak Jauh	Menetapkan dan mendokumentasikan pembatasan penggunaan, persyaratan konfigurasi/koneksi, dan panduan implementasi untuk setiap jenis akses jarak jauh yang diizinkan; dan Otorisasi setiap jenis akses jarak jauh ke sistem sebelum mengizinkan koneksi tersebut.	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositori data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.
AT-1: Kesadaran dan Pelatihan	Memberikan pelatihan literasi keamanan dan privasi kepada pengguna sistem (termasuk manajer, eksekutif senior, dan kontraktor)	security-awareness-program-exists(Pemeriksaan Proses)	Membangun dan memelihara program kesadaran keamanan untuk organisasi Anda. Program kesadaran keamanan mendidik karyawan tentang cara melindungi organisasi mereka dari berbagai pelanggaran atau insiden keamanan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2: Acara Audit	Identifikasi jenis-jenis peristiwa yang dapat dicatat oleh sistem untuk mendukung fungsi audit	audit-log-policy-exists(Pemeriksaan Proses)	Menetapkan dan memelihara kebijakan manajemen log audit yang menentukan persyaratan pencatatan organisasi Anda. Ini termasuk, namun tidak terbatas pada, peninjauan dan retensi log audit.
AU-16: Pencatatan Audit Lintas Organisasi	Menggunakan metode yang ditentukan lembaga untuk mengoordinasikan informasi audit yang ditentukan lembaga di antara organisasi eksternal ketika informasi audit ditransmisikan melintasi batas-batas organisasi.	audit-log-policy-exists(Pemeriksaan Proses)	Menetapkan dan memelihara kebijakan manajemen log audit yang menentukan persyaratan pencatatan organisasi Anda. Ini termasuk, namun tidak terbatas pada, peninjauan dan retensi log audit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7: Pemantauan Berkelanjutan	Mengembangkan strategi pemantaua n berkelanjutan tingkat sistem dan menerapkan pemantauan berkelanj utan sesuai dengan strategi pemantaua n berkelanjutan tingkat organisasi: Menetapkan metrik yang ditentuka n lembaga untuk dipantau; Penilaian kontrol berkelanj utan sesuai dengan strategi pemantaua n berkelanjutan; Pemantauan berkelanjutan dari metrik sistem dan organisasi yang ditentukan sesuai dengan strategi pemantauan berkelanj utan; Korelasi dan analisis informasi yang dihasilkan oleh penilaian dan pemantauan kontrol; Tindakan respons untuk mengatasi hasil analisis kontrol penilaian dan	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	pemantauan informasi ; dan Melaporkan status keamanan dan privasi sistem kepada personel yang ditentukan lembaga setiap tahun, minimal.		
CP-9: Sistem Backup	a. Melakukan backup informasi tingkat pengguna yang terkandung dalam dokumenta si sistem, termasuk dokumentasi terkait keamanan, mingguan; b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem mingguan; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumenta si terkait keamanan dan privasi setiap minggu; dan d. Melindungi kerahasia an, integritas, dan ketersediaan informasi cadangan.	aurora-resources-p rotected-by-rencana cadangan	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9: Sistem Backup	a. Melakukan backup informasi tingkat pengguna yang terkandung dalam dokumentasi sistem, termasuk dokumentasi terkait keamanan, mingguan; b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem mingguan; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumentasi terkait keamanan dan privasi setiap minggu; dan d. Melindungi kerahasiaan, integritas, dan ketersediaan informasi cadangan.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9: Sistem Backup	a. Melakukan backup informasi tingkat pengguna yang terkandung dalam dokumenta si sistem, termasuk dokumentasi terkait keamanan, mingguan; b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem mingguan; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumenta si terkait keamanan dan privasi setiap minggu; dan d. Melindungi kerahasia an, integritas, dan ketersediaan informasi cadangan.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9: Sistem Backup	a. Melakukan backup informasi tingkat pengguna yang terkandung dalam dokumentasi sistem, termasuk dokumentasi terkait keamanan, mingguan; b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem mingguan; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumentasi terkait keamanan dan privasi setiap minggu; dan d. Melindungi kerahasiaan, integritas, dan ketersediaan informasi cadangan.	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9: Sistem Backup	a. Melakukan backup informasi tingkat pengguna yang terkandung dalam dokumentasi sistem, termasuk dokumentasi terkait keamanan, mingguan; b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem mingguan; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumentasi terkait keamanan dan privasi setiap minggu; dan d. Melindungi kerahasiaan, integritas, dan ketersediaan informasi cadangan.	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9: Sistem Backup	a. Melakukan backup informasi tingkat pengguna yang terkandung dalam dokumenta si sistem, termasuk dokumentasi terkait keamanan, mingguan; b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem mingguan; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumenta si terkait keamanan dan privasi setiap minggu; dan d. Melindungi kerahasia an, integritas, dan ketersediaan informasi cadangan.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9: Sistem Backup	a. Melakukan backup informasi tingkat pengguna yang terkandung dalam dokumentasi sistem, termasuk dokumentasi terkait keamanan, mingguan; b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem mingguan; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumentasi terkait keamanan dan privasi setiap minggu; dan d. Melindungi kerahasiaan, integritas, dan ketersediaan informasi cadangan.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9: Sistem Backup	a. Melakukan backup informasi tingkat pengguna yang terkandung dalam dokumentasi sistem, termasuk dokumentasi terkait keamanan, mingguan; b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem mingguan; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumentasi terkait keamanan dan privasi setiap minggu; dan d. Melindungi kerahasiaan, integritas, dan ketersediaan informasi cadangan.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9: Sistem Backup	a. Melakukan backup informasi tingkat pengguna yang terkandung dalam dokumenta si sistem, termasuk dokumentasi terkait keamanan, mingguan; b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem mingguan; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumenta si terkait keamanan dan privasi setiap minggu; dan d. Melindungi kerahasia an, integritas, dan ketersediaan informasi cadangan.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9: Sistem Backup	a. Melakukan backup informasi tingkat pengguna yang terkandung dalam dokumenta si sistem, termasuk dokumentasi terkait keamanan, mingguan; b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem mingguan; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumenta si terkait keamanan dan privasi setiap minggu; dan d. Melindungi kerahasia an, integritas, dan ketersediaan informasi cadangan.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9: Sistem Backup	a. Melakukan backup informasi tingkat pengguna yang terkandung dalam dokumentasi sistem, termasuk dokumentasi terkait keamanan, mingguan; b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem mingguan; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumentasi terkait keamanan dan privasi setiap minggu; dan d. Melindungi kerahasiaan, integritas, dan ketersediaan informasi cadangan.	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9: Sistem Backup	a. Melakukan backup informasi tingkat pengguna yang terkandung dalam dokumenta si sistem, termasuk dokumentasi terkait keamanan, mingguan; b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem mingguan; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumenta si terkait keamanan dan privasi setiap minggu; dan d. Melindungi kerahasia an, integritas, dan ketersediaan informasi cadangan.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9: Sistem Backup	a. Melakukan backup informasi tingkat pengguna yang terkandung dalam dokumenta si sistem, termasuk dokumentasi terkait keamanan, mingguan; b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem mingguan; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumenta si terkait keamanan dan privasi setiap minggu; dan d. Melindungi kerahasia an, integritas, dan ketersediaan informasi cadangan.	fsx-resources-prot ected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9: Sistem Backup	a. Melakukan backup informasi tingkat pengguna yang terkandung dalam dokumenta si sistem, termasuk dokumentasi terkait keamanan, mingguan; b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem mingguan; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumenta si terkait keamanan dan privasi setiap minggu; dan d. Melindungi kerahasia an, integritas, dan ketersediaan informasi cadangan.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9: Sistem Backup	a. Melakukan backup informasi tingkat pengguna yang terkandung dalam dokumentasi sistem, termasuk dokumentasi terkait keamanan, mingguan; b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem mingguan; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumentasi terkait keamanan dan privasi setiap minggu; dan d. Melindungi kerahasiaan, integritas, dan ketersediaan informasi cadangan.	rds-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Relational Database Service (Amazon RDS) Anda merupakan AWS bagian dari paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9: Sistem Backup	a. Melakukan backup informasi tingkat pengguna yang terkandung dalam dokumentasi sistem, termasuk dokumentasi terkait keamanan, mingguan; b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem mingguan; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumentasi terkait keamanan dan privasi setiap minggu; dan d. Melindungi kerahasiaan, integritas, dan ketersediaan informasi cadangan.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9: Sistem Backup	a. Melakukan backup informasi tingkat pengguna yang terkandung dalam dokumenta si sistem, termasuk dokumentasi terkait keamanan, mingguan; b. Melakukan backup informasi tingkat sistem yang terkandung dalam sistem mingguan; c. Melakukan pencadangan dokumentasi sistem, termasuk dokumenta si terkait keamanan dan privasi setiap minggu; dan d. Melindungi kerahasia an, integritas, dan ketersediaan informasi cadangan.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2: Identifikasi dan Otentikasi (Pengguna Organisasi) (CE-1) Otentikasi Multifaktor ke Akun Istimewa	Menerapkan otentikasi multi-faktor untuk akses ke akun istimewa	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2: Identifikasi dan Otentikasi (Pengguna Organisasi) (CE-1) Otentikasi Multifaktor ke Akun Istimewa	Menerapkan otentikasi multi-faktor untuk akses ke akun istimewa	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2: Identifikasi dan Otentikasi (Pengguna Organisasi) (CE-2) Otentikasi Multifaktor ke Akun Non-Istimewa	Menerapkan otentikasi multi-faktor untuk akses ke akun yang tidak memiliki hak istimewa.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-5: Manajemen Authenticator: (CE-1) Otentikasi Berbasis Kata Sandi: Untuk otentikasi berbasis kata sandi	Menegakkan aturan komposisi dan kompleksitas berikut: 1. Menerapkan panjang kata sandi minimum empat belas (14) karakter. 2. Menegakkan kompleksitas kata sandi minimum untuk berisi kombinasi angka, huruf besar, huruf kecil, dan karakter khusus. 3. Terapkan setidakny a satu (1) perubahan karakter saat kata sandi baru dipilih untuk digunakan . 4. Simpan dan kirimkan hanya kata sandi yang dilindung i secara kriptogra fi. 5. Menegakka n batasan seumur hidup kata sandi: i. Minimal satu (1) hari dan maksimum 90 hari. ii. Kata sandi akun layanan akan kedaluwarsa dalam 366 hari (inklusif).	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifik asi berdasark an kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkin kan Anda untuk mengatur secara opsional RequireUp percaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PM-5: Inventaris Sistem	Mengembangkan dan memperbarui inventaris sistem organisasi secara terus menerus.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PM-5: Inventaris Sistem	Mengembangkan dan memperbarui inventaris sistem organisasi secara terus menerus.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PM-5: Inventaris Sistem	Mengembangkan dan memperbarui inventaris sistem organisasi secara terus menerus.	vpc-network-acl-unused-periksa	Aturan ini memastikan bahwa daftar kontrol akses jaringan Amazon Virtual Private Cloud (VPC) sedang digunakan. Pemantauan untuk daftar kontrol akses jaringan yang tidak digunakan dapat membantu inventaris dan pengelolaan lingkungan Anda yang akurat.
PM-5: Inventaris Sistem	Mengembangkan dan memperbarui inventaris sistem organisasi secara terus menerus.	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RA-5: Pemantauan dan Pemindaian Kerentanan	Memantau dan memindai kerentanan dalam sistem dan aplikasi yang di-host setiap tiga puluh (30) hari, sebelum menempatkan sistem informasi baru di jaringan agensi, untuk mengkonfirmasi tindakan perbaikan, dan ketika kerentanan baru yang berpotensi mempengaruhi sistem diidentifikasi dan dilaporkan	vuln-scans-performed(Pemeriksaan Proses)	Pastikan pemindaian kerentanan dilakukan sesuai dengan persyaratan kepatuhan Anda. Irama pemindaian, alat yang digunakan, dan penggunaan hasil harus ditentukan oleh organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-10: Manajemen Konfigurasi Pengembang (e.)	Lacak kelemahan keamanan dan resolusi cacat dalam sistem, komponen, atau layanan dan laporkan temuan ke [Penugasan: personel yang ditentukan organisasi].	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-10: Manajemen Konfigurasi Pengembang (e.)	Lacak kelemahan keamanan dan resolusi cacat dalam sistem, komponen, atau layanan dan laporkan temuan ke [Penugasan: personel yang ditentukan organisasi].	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-10: Manajemen Konfigurasi Pengembang (e.)	Lacak kelemahan keamanan dan resolusi cacat dalam sistem, komponen, atau layanan dan laporkan temuan ke [Penugasan: personel yang ditentukan organisasi].	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-10: Manajemen Konfigurasi Pengembang (a) (c.)	Melakukan manajemen konfigura si selama desain sistem, komponen, atau layanan, pengembangan, implementasi, operasi; Menerapka n hanya perubahan yang disetujui organisasi pada sistem, komponen, atau layanan;	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-4: Informasi dalam Sumber Daya Sistem Bersama	Mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7: Perlindungan Batas	Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; Menerapkan subnetwork untuk komponen sistem yang dapat diakses publik yang terpisah dari jaringan organisasi internal; dan Connect ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7: Perlindungan Batas	Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; Menerapkan subnetwork untuk komponen sistem yang dapat diakses publik yang terpisah dari jaringan organisasi internal; dan Connect ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7: Perlindungan Batas	Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; Menerapkan subnetwork untuk komponen sistem yang dapat diakses publik yang terpisah dari jaringan organisasi internal; dan Connect ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7: Perlindungan Batas	Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; Menerapkan subnetwork untuk komponen sistem yang dapat diakses publik yang terpisah dari jaringan organisasi internal; dan Connect ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7: Perlindungan Batas	Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; Menerapkan subnetwork untuk komponen sistem yang dapat diakses publik yang terpisah dari jaringan organisasi internal; dan Connect ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7: Perlindungan Batas	Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; Menerapkan subnetwork untuk komponen sistem yang dapat diakses publik yang terpisah dari jaringan organisasi internal; dan Connect ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7: Perlindungan Batas	Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; Menerapkan subnetwork untuk komponen sistem yang dapat diakses publik yang terpisah dari jaringan organisasi internal; dan Connect ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7: Perlindungan Batas	Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; Menerapkan subnetwork untuk komponen sistem yang dapat diakses publik yang terpisah dari jaringan organisasi internal; dan Connect ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7: Perlindungan Batas	Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; Menerapkan subnetwork untuk komponen sistem yang dapat diakses publik yang terpisah dari jaringan organisasi internal; dan Connect ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7: Perlindungan Batas	Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; Menerapkan subnetwork untuk komponen sistem yang dapat diakses publik yang terpisah dari jaringan organisasi internal; dan Connect ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7: Perlindungan Batas	Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; Menerapkan subnetwork untuk komponen sistem yang dapat diakses publik yang terpisah dari jaringan organisasi internal; dan Connect ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7: Perlindungan Batas	Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; Menerapkan subnetwork untuk komponen sistem yang dapat diakses publik yang terpisah dari jaringan organisasi internal; dan Connect ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7: Perlindungan Batas (CE-9) Membatasi Lalu Lintas Komunikasi Keluar yang Mengancam	Mendeteksi dan menolak lalu lintas komunikasi keluar yang menimbulkan ancaman bagi sistem eksternal; dan Audit identitas pengguna internal yang terkait dengan komunikasi yang ditolak.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7: Perlindungan Batas (CE-9) Membatasi Lalu Lintas Komunikasi Keluar yang Mengancam	Mendeteksi dan menolak lalu lintas komunikasi keluar yang menimbulkan ancaman bagi sistem eksternal; dan Audit identitas pengguna internal yang terkait dengan komunikasi yang ditolak.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7: Perlindungan Batas (CE-9) Membatasi Lalu Lintas Komunikasi Keluar yang Mengancam	Mendeteksi dan menolak lalu lintas komunikasi keluar yang menimbulkan ancaman bagi sistem eksternal; dan Audit identitas pengguna internal yang terkait dengan komunikasi yang ditolak.	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindungi nya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7: Perlindungan Batas (ditentukan IRS)	Agensi harus menerapkan dan mengelola perlindun gan batas (biasanya menggunakan firewall) pada batas kepercayaan. Setiap batas kepercayaan harus dipantau dan komunikasi di setiap batas harus dikendali kan.	netfw-policy-rule-group-terkait	Kebijakan AWS Network Firewall mendefinisikan bagaimana firewall Anda memantau dan menangani lalu lintas di VPC Amazon. Anda mengonfigurasi grup aturan stateless dan stateful untuk memfilter paket dan arus lalu lintas, dan Anda menentuka n penanganan lalu lintas default.
SC-7: Perlindungan Batas (ditentukan IRS)	Agensi harus menerapkan dan mengelola perlindun gan batas (biasanya menggunakan firewall) pada batas kepercayaan. Setiap batas kepercayaan harus dipantau dan komunikasi di setiap batas harus dikendali kan.	netfw-stateless-rule-group-tidak-kosong	Grup aturan AWS Network Firewall berisi aturan yang menentukan bagaimana firewall Anda memproses lalu lintas di VPC Anda. Grup aturan stateless kosong saat ada dalam kebijakan firewall tidak memproses lalu lintas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8: Perlindungan Kriptografi dan Kerahasiaan Transmisi (CE-1)	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan informasi yang tidak sah dan mendeteksi perubahan informasi selama transmisi.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-8: Perlindungan Kriptografi dan Kerahasiaan Transmisi (CE-1)	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan informasi yang tidak sah dan mendeteksi perubahan informasi selama transmisi.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8: Perlindungan Kriptografi dan Kerahasiaan Transmisi (CE-1)	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan informasi yang tidak sah dan mendeteksi perubahan informasi selama transmisi.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-8: Perlindungan Kriptografi dan Kerahasiaan Transmisi (CE-1)	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan informasi yang tidak sah dan mendeteksi perubahan informasi selama transmisi.	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8: Perlindungan Kriptografi dan Kerahasiaan Transmisi (CE-1)	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan informasi yang tidak sah dan mendeteksi perubahan informasi selama transmisi.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-8: Perlindungan Kriptografi dan Kerahasiaan Transmisi (CE-1)	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan informasi yang tidak sah dan mendeteksi perubahan informasi selama transmisi.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8: Perlindungan Kriptografi dan Kerahasiaan Transmisi (CE-1)	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan informasi yang tidak sah dan mendeteksi perubahan informasi selama transmisi.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-12: Pembentukan dan Manajemen Kunci Kriptografi	Agensi harus menetapkan dan mengelola kunci kriptografi ketika kriptografi digunakan dalam sistem sesuai dengan persyarat an manajemen kunci berikut: NIST SP 800-57, Rekomendasi untuk Manajemen Kunci, untuk pembuatan kunci, distribusi, penyimpanan, akses, dan penghancuran.	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-12: Pembentukan dan Manajemen Kunci Kriptografi	Agensi harus menetapkan dan mengelola kunci kriptografi ketika kriptografi digunakan dalam sistem sesuai dengan persyarat an manajemen kunci berikut: NIST SP 800-57, Rekomendasi untuk Manajemen Kunci, untuk pembuatan kunci, distribusi, penyimpanan, akses, dan penghancuran.	cmk-backing-key-ro tation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13: Perlindungan Kriptografi	Menerapkan jenis kriptografi berikut yang diperluka n untuk setiap penggunaan kriptogra fi yang ditentukan: Mekanisme enkripsi tervalidasi FIPS-140 terbaru, NIST 800-52, Guidelines for the Selection, Configura tion, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 untuk tanda tangan digital dilarang.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13: Perlindungan Kriptografi	Menerapkan jenis kriptografi berikut yang diperluka n untuk setiap penggunaan kriptogra fi yang ditentukan: Mekanisme enkripsi tervalidasi FIPS-140 terbaru, NIST 800-52, Guidelines for the Selection, Configura tion, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 untuk tanda tangan digital dilarang.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13: Perlindungan Kriptografi	Menerapkan jenis kriptografi berikut yang diperluka n untuk setiap penggunaan kriptogra fi yang ditentukan: Mekanisme enkripsi tervalidasi FIPS-140 terbaru, NIST 800-52, Guidelines for the Selection, Configura tion, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 untuk tanda tangan digital dilarang.	api-gw-cache-enabl ed-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13: Perlindungan Kriptografi	Menerapkan jenis kriptografi berikut yang diperluka n untuk setiap penggunaan kriptogra fi yang ditentukan: Mekanisme enkripsi tervalidasi FIPS-140 terbaru, NIST 800-52, Guidelines for the Selection, Configura tion, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 untuk tanda tangan digital dilarang.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-n ode enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkrip si memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13: Perlindungan Kriptografi	Menerapkan jenis kriptografi berikut yang diperluka n untuk setiap penggunaan kriptogra fi yang ditentukan: Mekanisme enkripsi tervalidasi FIPS-140 terbaru, NIST 800-52, Guidelines for the Selection, Configura tion, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 untuk tanda tangan digital dilarang.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13: Perlindungan Kriptografi	Menerapkan jenis kriptografi berikut yang diperluka n untuk setiap penggunaan kriptogra fi yang ditentukan: Mekanisme enkripsi tervalidasi FIPS-140 terbaru, NIST 800-52, Guidelines for the Selection, Configura tion, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 untuk tanda tangan digital dilarang.	opensearch-https-r equired	Karena data sensitif dapat ada dan membantu melindung i data dalam perjalana n, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13: Perlindungan Kriptografi	Menerapkan jenis kriptografi berikut yang diperluka n untuk setiap penggunaan kriptogra fi yang ditentukan: Mekanisme enkripsi tervalidasi FIPS-140 terbaru, NIST 800-52, Guidelines for the Selection, Configura tion, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 untuk tanda tangan digital dilarang.	opensearch-node-to -node-pemeriksaan enkripsi-	Pastikan node-to-n ode enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkrip si memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13: Perlindungan Kriptografi	Menerapkan jenis kriptografi berikut yang diperluka n untuk setiap penggunaan kriptogra fi yang ditentukan: Mekanisme enkripsi tervalidasi FIPS-140 terbaru, NIST 800-52, Guidelines for the Selection, Configura tion, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 untuk tanda tangan digital dilarang.	backup-recovery-po int-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13: Perlindungan Kriptografi	Menerapkan jenis kriptografi berikut yang diperluka n untuk setiap penggunaan kriptogra fi yang ditentukan: Mekanisme enkripsi tervalidasi FIPS-140 terbaru, NIST 800-52, Guidelines for the Selection, Configura tion, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 untuk tanda tangan digital dilarang.	dynamodb-table-enc rypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindung i data tersebut. Secara default, tabel DynamoDB dienkrips i dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13: Perlindungan Kriptografi	Menerapkan jenis kriptografi berikut yang diperluka n untuk setiap penggunaan kriptogra fi yang ditentukan: Mekanisme enkripsi tervalidasi FIPS-140 terbaru, NIST 800-52, Guidelines for the Selection, Configura tion, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 untuk tanda tangan digital dilarang.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13: Perlindungan Kriptografi	Menerapkan jenis kriptografi berikut yang diperlukan untuk setiap penggunaan kriptografi yang ditentukan: Mekanisme enkripsi tervalidasi FIPS-140 terbaru, NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 untuk tanda tangan digital dilarang.	kinesis-stream-encrypted	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13: Perlindungan Kriptografi	Menerapkan jenis kriptografi berikut yang diperluka n untuk setiap penggunaan kriptogra fi yang ditentukan: Mekanisme enkripsi tervalidasi FIPS-140 terbaru, NIST 800-52, Guidelines for the Selection, Configura tion, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 untuk tanda tangan digital dilarang.	opensearch-encrypt ed-at-rest	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk domain OpenSearc h Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13: Perlindungan Kriptografi	Menerapkan jenis kriptografi berikut yang diperluka n untuk setiap penggunaan kriptogra fi yang ditentukan: Mekanisme enkripsi tervalidasi FIPS-140 terbaru, NIST 800-52, Guidelines for the Selection, Configura tion, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 untuk tanda tangan digital dilarang.	rds-snapshot-encry pted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13: Perlindungan Kriptografi	Menerapkan jenis kriptografi berikut yang diperluka n untuk setiap penggunaan kriptogra fi yang ditentukan: Mekanisme enkripsi tervalidasi FIPS-140 terbaru, NIST 800-52, Guidelines for the Selection, Configura tion, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 untuk tanda tangan digital dilarang.	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13: Perlindungan Kriptografi	Menerapkan jenis kriptografi berikut yang diperluka n untuk setiap penggunaan kriptogra fi yang ditentukan: Mekanisme enkripsi tervalidasi FIPS-140 terbaru, NIST 800-52, Guidelines for the Selection, Configura tion, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 untuk tanda tangan digital dilarang.	s3- default-encryption -kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13: Perlindungan Kriptografi	Menerapkan jenis kriptografi berikut yang diperluka n untuk setiap penggunaan kriptogra fi yang ditentukan: Mekanisme enkripsi tervalidasi FIPS-140 terbaru, NIST 800-52, Guidelines for the Selection, Configura tion, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 untuk tanda tangan digital dilarang.	secretsmanager-usi ng-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13: Perlindungan Kriptografi	Menerapkan jenis kriptografi berikut yang diperluka n untuk setiap penggunaan kriptogra fi yang ditentukan: Mekanisme enkripsi tervalidasi FIPS-140 terbaru, NIST 800-52, Guidelines for the Selection, Configura tion, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 untuk tanda tangan digital dilarang.	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13: Perlindungan Kriptografi	Menerapkan jenis kriptografi berikut yang diperluka n untuk setiap penggunaan kriptogra fi yang ditentukan: Mekanisme enkripsi tervalidasi FIPS-140 terbaru, NIST 800-52, Guidelines for the Selection, Configura tion, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 untuk tanda tangan digital dilarang.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13: Perlindungan Kriptografi	Menerapkan jenis kriptografi berikut yang diperlukan untuk setiap penggunaan kriptografi yang ditentukan: Mekanisme enkripsi tervalidasi FIPS-140 terbaru, NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 untuk tanda tangan digital dilarang.	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13: Perlindungan Kriptografi	Menerapkan jenis kriptografi berikut yang diperluka n untuk setiap penggunaan kriptogra fi yang ditentukan: Mekanisme enkripsi tervalidasi FIPS-140 terbaru, NIST 800-52, Guidelines for the Selection, Configura tion, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 untuk tanda tangan digital dilarang.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13: Perlindungan Kriptografi	Menerapkan jenis kriptografi berikut yang diperluka n untuk setiap penggunaan kriptogra fi yang ditentukan: Mekanisme enkripsi tervalidasi FIPS-140 terbaru, NIST 800-52, Guidelines for the Selection, Configura tion, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 untuk tanda tangan digital dilarang.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13: Perlindungan Kriptografi	Menerapkan jenis kriptografi berikut yang diperlukan untuk setiap penggunaan kriptografi yang ditentukan: Mekanisme enkripsi tervalidasi FIPS-140 terbaru, NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 untuk tanda tangan digital dilarang.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13: Perlindungan Kriptografi	Menerapkan jenis kriptografi berikut yang diperluka n untuk setiap penggunaan kriptogra fi yang ditentukan: Mekanisme enkripsi tervalidasi FIPS-140 terbaru, NIST 800-52, Guidelines for the Selection, Configura tion, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 untuk tanda tangan digital dilarang.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13: Perlindungan Kriptografi	Menerapkan jenis kriptografi berikut yang diperluka n untuk setiap penggunaan kriptogra fi yang ditentukan: Mekanisme enkripsi tervalidasi FIPS-140 terbaru, NIST 800-52, Guidelines for the Selection, Configura tion, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 untuk tanda tangan digital dilarang.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13: Perlindungan Kriptografi	Menerapkan jenis kriptografi berikut yang diperluka n untuk setiap penggunaan kriptogra fi yang ditentukan: Mekanisme enkripsi tervalidasi FIPS-140 terbaru, NIST 800-52, Guidelines for the Selection, Configura tion, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 untuk tanda tangan digital dilarang.	s3- bucket-ssl-request s-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13: Perlindungan Kriptografi	Menerapkan jenis kriptografi berikut yang diperluka n untuk setiap penggunaan kriptogra fi yang ditentukan: Mekanisme enkripsi tervalidasi FIPS-140 terbaru, NIST 800-52, Guidelines for the Selection, Configura tion, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 untuk tanda tangan digital dilarang.	sagemaker-endpoint -configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13: Perlindungan Kriptografi	Menerapkan jenis kriptografi berikut yang diperluka n untuk setiap penggunaan kriptogra fi yang ditentukan: Mekanisme enkripsi tervalidasi FIPS-140 terbaru, NIST 800-52, Guidelines for the Selection, Configura tion, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 untuk tanda tangan digital dilarang.	sagemaker-notebook -instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13: Perlindungan Kriptografi	Menerapkan jenis kriptografi berikut yang diperluka n untuk setiap penggunaan kriptogra fi yang ditentukan: Mekanisme enkripsi tervalidasi FIPS-140 terbaru, NIST 800-52, Guidelines for the Selection, Configura tion, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 untuk tanda tangan digital dilarang.	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-23: Keaslian Sesi	Lindungi keaslian sesi komunikasi.	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28: Perlindungan Informasi Saat Istirahat (CE-1) Perlindungan Kriptografi	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi FTI yang tidak sah pada sistem komputasi pengguna akhir (yaitu, komputer desktop, komputer laptop, perangkat seluler, perangkat penyimpanan portabel dan dapat dilepas) dalam penyimpanan yang tidak mudah menguap.	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-28: Perlindungan Informasi Saat Istirahat (CE-1) Perlindungan Kriptografi	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi FTI yang tidak sah pada sistem komputasi pengguna akhir (yaitu, komputer desktop, komputer laptop, perangkat seluler, perangkat penyimpanan portabel dan dapat dilepas) dalam penyimpanan yang tidak mudah menguap.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28: Perlindungan Informasi Saat Istirahat (CE-1) Perlindungan Kriptografi	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi FTI yang tidak sah pada sistem komputasi pengguna akhir (yaitu, komputer desktop, komputer laptop, perangkat seluler, perangkat penyimpanan portabel dan dapat dilepas) dalam penyimpanan yang tidak mudah menguap.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
SC-28: Perlindungan Informasi Saat Istirahat (CE-1) Perlindungan Kriptografi	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi FTI yang tidak sah pada sistem komputasi pengguna akhir (yaitu, komputer desktop, komputer laptop, perangkat seluler, perangkat penyimpanan portabel dan dapat dilepas) dalam penyimpanan yang tidak mudah menguap.	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28: Perlindungan Informasi Saat Istirahat (CE-1) Perlindungan Kriptografi	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi FTI yang tidak sah pada sistem komputasi pengguna akhir (yaitu, komputer desktop, komputer laptop, perangkat seluler, perangkat penyimpanan portabel dan dapat dilepas) dalam penyimpanan yang tidak mudah menguap.	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28: Perlindungan Informasi Saat Istirahat (CE-1) Perlindungan Kriptografi	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi FTI yang tidak sah pada sistem komputasi pengguna akhir (yaitu, komputer desktop, komputer laptop, perangkat seluler, perangkat penyimpanan portabel dan dapat dilepas) dalam penyimpanan yang tidak mudah menguap.	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
SC-28: Perlindungan Informasi Saat Istirahat (CE-1) Perlindungan Kriptografi	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi FTI yang tidak sah pada sistem komputasi pengguna akhir (yaitu, komputer desktop, komputer laptop, perangkat seluler, perangkat penyimpanan portabel dan dapat dilepas) dalam penyimpanan yang tidak mudah menguap.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28: Perlindungan Informasi Saat Istirahat (CE-1) Perlindungan Kriptografi	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi FTI yang tidak sah pada sistem komputasi pengguna akhir (yaitu, komputer desktop, komputer laptop, perangkat seluler, perangkat penyimpanan portabel dan dapat dilepas) dalam penyimpanan yang tidak mudah menguap.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
SC-28: Perlindungan Informasi Saat Istirahat (CE-1) Perlindungan Kriptografi	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi FTI yang tidak sah pada sistem komputasi pengguna akhir (yaitu, komputer desktop, komputer laptop, perangkat seluler, perangkat penyimpanan portabel dan dapat dilepas) dalam penyimpanan yang tidak mudah menguap.	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28: Perlindungan Informasi Saat Istirahat (CE-1) Perlindungan Kriptografi	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi FTI yang tidak sah pada sistem komputasi pengguna akhir (yaitu, komputer desktop, komputer laptop, perangkat seluler, perangkat penyimpanan portabel dan dapat dilepas) dalam penyimpanan yang tidak mudah menguap.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
SC-28: Perlindungan Informasi Saat Istirahat (CE-1) Perlindungan Kriptografi	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi FTI yang tidak sah pada sistem komputasi pengguna akhir (yaitu, komputer desktop, komputer laptop, perangkat seluler, perangkat penyimpanan portabel dan dapat dilepas) dalam penyimpanan yang tidak mudah menguap.	kinesis-stream-encrypted	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28: Perlindungan Informasi Saat Istirahat (CE-1) Perlindungan Kriptografi	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi FTI yang tidak sah pada sistem komputasi pengguna akhir (yaitu, komputer desktop, komputer laptop, perangkat seluler, perangkat penyimpanan portabel dan dapat dilepas) dalam penyimpanan yang tidak mudah menguap.	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
SC-28: Perlindungan Informasi Saat Istirahat (CE-1) Perlindungan Kriptografi	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi FTI yang tidak sah pada sistem komputasi pengguna akhir (yaitu, komputer desktop, komputer laptop, perangkat seluler, perangkat penyimpanan portabel dan dapat dilepas) dalam penyimpanan yang tidak mudah menguap.	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28: Perlindungan Informasi Saat Istirahat (CE-1) Perlindungan Kriptografi	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi FTI yang tidak sah pada sistem komputasi pengguna akhir (yaitu, komputer desktop, komputer laptop, perangkat seluler, perangkat penyimpanan portabel dan dapat dilepas) dalam penyimpanan yang tidak mudah menguap.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28: Perlindungan Informasi Saat Istirahat (CE-1) Perlindungan Kriptografi	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi FTI yang tidak sah pada sistem komputasi pengguna akhir (yaitu, komputer desktop, komputer laptop, perangkat seluler, perangkat penyimpanan portabel dan dapat dilepas) dalam penyimpanan yang tidak mudah menguap.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28: Perlindungan Informasi Saat Istirahat (CE-1) Perlindungan Kriptografi	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi FTI yang tidak sah pada sistem komputasi pengguna akhir (yaitu, komputer desktop, komputer laptop, perangkat seluler, perangkat penyimpanan portabel dan dapat dilepas) dalam penyimpanan yang tidak mudah menguap.	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-28: Perlindungan Informasi Saat Istirahat (CE-1) Perlindungan Kriptografi	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi FTI yang tidak sah pada sistem komputasi pengguna akhir (yaitu, komputer desktop, komputer laptop, perangkat seluler, perangkat penyimpanan portabel dan dapat dilepas) dalam penyimpanan yang tidak mudah menguap.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28: Perlindungan Informasi Saat Istirahat (CE-1) Perlindungan Kriptografi	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi FTI yang tidak sah pada sistem komputasi pengguna akhir (yaitu, komputer desktop, komputer laptop, perangkat seluler, perangkat penyimpanan portabel dan dapat dilepas) dalam penyimpanan yang tidak mudah menguap.	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-28: Perlindungan Informasi Saat Istirahat (CE-1) Perlindungan Kriptografi	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi FTI yang tidak sah pada sistem komputasi pengguna akhir (yaitu, komputer desktop, komputer laptop, perangkat seluler, perangkat penyimpanan portabel dan dapat dilepas) dalam penyimpanan yang tidak mudah menguap.	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28: Perlindungan Informasi Saat Istirahat (CE-1) Perlindungan Kriptografi	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi FTI yang tidak sah pada sistem komputasi pengguna akhir (yaitu, komputer desktop, komputer laptop, perangkat seluler, perangkat penyimpanan portabel dan dapat dilepas) dalam penyimpanan yang tidak mudah menguap.	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-28: Perlindungan Informasi Saat Istirahat (CE-1) Perlindungan Kriptografi	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan dan modifikasi FTI yang tidak sah pada sistem komputasi pengguna akhir (yaitu, komputer desktop, komputer laptop, perangkat seluler, perangkat penyimpanan portabel dan dapat dilepas) dalam penyimpanan yang tidak mudah menguap.	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2: Remediasi Cacat (didefinisikan IRS)	Agensi harus memastikan bahwa, setelah power up harian dan koneksi ke jaringan agensi, workstati on (sebagaimana didefinisikan dalam kebijakan dan termasuk koneksi jarak jauh menggunak an workstation GFE) diperiksa untuk memastikan bahwa patch terbaru yang disetujui agensi telah diterapkan dan bahwa patch yang tidak ada atau baru diterapka n seperlunya atau diperiksa tidak kurang dari setelah setiap 24 jam (tidak termasuk akhir pekan, hari libur, dll.)	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2: Remediasi Cacat (didefinisikan IRS)	Agensi harus memastikan bahwa, setelah power up harian dan koneksi ke jaringan agensi, workstati on (sebagaimana didefinisikan dalam kebijakan dan termasuk koneksi jarak jauh menggunak an workstation GFE) diperiksa untuk memastikan bahwa patch terbaru yang disetujui agensi telah diterapkan dan bahwa patch yang tidak ada atau baru diterapka n seperlunya atau diperiksa tidak kurang dari setelah setiap 24 jam (tidak termasuk akhir pekan, hari libur, dll.)	ec2- -periksa managedinstance-as sociation-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventari s platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2: Remediasi Cacat (didefinisikan IRS)	Agensi harus memastikan bahwa, setelah power up harian dan koneksi ke jaringan agensi, workstati on (sebagaimana didefinisikan dalam kebijakan dan termasuk koneksi jarak jauh menggunak an workstation GFE) diperiksa untuk memastikan bahwa patch terbaru yang disetujui agensi telah diterapkan dan bahwa patch yang tidak ada atau baru diterapka n seperlunya atau diperiksa tidak kurang dari setelah setiap 24 jam (tidak termasuk akhir pekan, hari libur, dll.)	ec2- -periksa managedinstance-pa tch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2: Remediasi Cacat (didefinisikan IRS)	Agensi harus memastikan bahwa, setelah power up harian dan koneksi ke jaringan agensi, workstati on (sebagaimana didefinisikan dalam kebijakan dan termasuk koneksi jarak jauh menggunak an workstation GFE) diperiksa untuk memastikan bahwa patch terbaru yang disetujui agensi telah diterapkan dan bahwa patch yang tidak ada atau baru diterapka n seperlunya atau diperiksa tidak kurang dari setelah setiap 24 jam (tidak termasuk akhir pekan, hari libur, dll.)	ecs-fargate-latest-platform-versi	Pembaruan dan tambalan keamanan diterapkan secara otomatis untuk tugas Fargate AWS Anda. Jika ditemukan masalah keamanan yang memengaru hi versi platform AWS Fargate, AWS tambal versi platform. Untuk membantu pengelolaan tambalan tugas Amazon Elastic Container Service (ECS) yang menjalank an AWS Fargate, perbarui tugas mandiri layanan Anda untuk menggunakan versi platform terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2: Remediasi Cacat (didefinisikan IRS)	Agensi harus memastikan bahwa, setelah power up harian dan koneksi ke jaringan agensi, workstati on (sebagaimana didefinisikan dalam kebijakan dan termasuk koneksi jarak jauh menggunak an workstation GFE) diperiksa untuk memastikan bahwa patch terbaru yang disetujui agensi telah diterapkan dan bahwa patch yang tidak ada atau baru diterapka n seperlunya atau diperiksa tidak kurang dari setelah setiap 24 jam (tidak termasuk akhir pekan, hari libur, dll.)	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2: Remediasi Cacat (didefinisikan IRS)	Agensi harus memastikan bahwa, setelah power up harian dan koneksi ke jaringan agensi, workstati on (sebagaimana didefinisikan dalam kebijakan dan termasuk koneksi jarak jauh menggunak an workstation GFE) diperiksa untuk memastikan bahwa patch terbaru yang disetujui agensi telah diterapkan dan bahwa patch yang tidak ada atau baru diterapka n seperlunya atau diperiksa tidak kurang dari setelah setiap 24 jam (tidak termasuk akhir pekan, hari libur, dll.)	rds-automatic-mino r-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relationa l Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastika n pembaruan versi minor terbaru ke Relational Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4: Pemantauan Sistem	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1.Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2.Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c.Menyebarkan perangkat pemantauan: 1. Secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan 2. Di lokasi ad hoc dalam sistem untuk melacak jenis transaksi tertentu yang menarik	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	bagi organisasi; d. Melindungi informasi yang diperoleh dari alat pemantauan intrusi dari akses, modifikasi, dan penghapusan yang tidak sah;		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4: Pemantauan Sistem	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1.Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2.Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c.Menyebarkan perangkat pemantauan: 1. Secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan 2. Di lokasi ad hoc dalam sistem untuk melacak jenis transaksi tertentu yang menarik	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	bagi organisasi; d. Melindungi informasi yang diperoleh dari alat pemantauan intrusi dari akses, modifikasi, dan penghapusan yang tidak sah;		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4: Pemantauan Sistem	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1.Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2.Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c.Menyebarkan perangkat pemantauan: 1. Secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan 2. Di lokasi ad hoc dalam sistem untuk melacak jenis transaksi tertentu yang menarik	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	bagi organisasi; d. Melindungi informasi yang diperoleh dari alat pemantauan intrusi dari akses, modifikasi, dan penghapusan yang tidak sah;		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4: Pemantauan Sistem	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1.Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2.Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c.Menyebarkan perangkat pemantauan: 1. Secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan 2. Di lokasi ad hoc dalam sistem untuk melacak jenis transaksi tertentu yang menarik	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	bagi organisasi; d. Melindungi informasi yang diperoleh dari alat pemantauan intrusi dari akses, modifikasi, dan penghapusan yang tidak sah;		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4: Pemantauan Sistem	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1.Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2.Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c.Menyebarkan perangkat pemantauan: 1. Secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan 2. Di lokasi ad hoc dalam sistem untuk melacak jenis transaksi tertentu yang menarik	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	bagi organisasi; d. Melindungi informasi yang diperoleh dari alat pemantauan intrusi dari akses, modifikasi, dan penghapusan yang tidak sah;		
SI-4: Pemantauan Sistem (ditentukan IRS)	Semua titik Akses Internet/portal harus menangkap dan menyimpan, setidaknya selama satu tahun, informasi header lalu lintas masuk dan keluar, dengan pengecualian koneksi Internet “anonim” yang disetujui, sebagaimana dapat disetujui oleh agensi CISO.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4: Pemantauan Sistem (ditentukan IRS)	Semua titik Akses Internet/portal harus menangkap dan menyimpan, setidaknya selama satu tahun, informasi header lalu lintas masuk dan keluar, dengan pengecualian koneksi Internet “anonim” yang disetujui, sebagaimana dapat disetujui oleh agensi CISO.	opensearch-audit-logging-enabled	Pastikan pencatatan audit diaktifkan di domain OpenSearch Layanan Amazon Anda. Pencatatan audit memungkinkan Anda melacak aktivitas pengguna di OpenSearch domain Anda, termasuk keberhasilan dan kegagalan otentikasi, permintaan, perubahan indeks OpenSearch, dan kueri penelusuran yang masuk.
SI-4: Pemantauan Sistem (ditentukan IRS)	Semua titik Akses Internet/portal harus menangkap dan menyimpan, setidaknya selama satu tahun, informasi header lalu lintas masuk dan keluar, dengan pengecualian koneksi Internet “anonim” yang disetujui, sebagaimana dapat disetujui oleh agensi CISO.	redshift-audit-logging-enabled	Untuk menangkap informasi tentang koneksi dan aktivitas pengguna di klaster Amazon Redshift, pastikan pencatatan audit diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4: Pemantauan Sistem (ditentukan IRS)	Semua titik Akses Internet/portal harus menangkap dan menyimpan, setidaknya selama satu tahun, informasi header lalu lintas masuk dan keluar, dengan pengecualian koneksi Internet “anonim” yang disetujui, sebagaimana dapat disetujui oleh agensi CISO.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4: Pemantauan Sistem (ditentukan IRS)	Semua titik Akses Internet/portal harus menangkap dan menyimpan, setidaknya selama satu tahun, informasi header lalu lintas masuk dan keluar, dengan pengecualian koneksi Internet “anonim” yang disetujui, sebagaimana dapat disetujui oleh agensi CISO.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4: Pemantauan Sistem (ditentukan IRS)	Semua titik Akses Internet/portal harus menangkap dan menyimpan, setidakny a selama satu tahun, informasi header lalu lintas masuk dan keluar, dengan pengecualian koneksi Internet “anonim” yang disetujui, sebagaimana dapat disetujui oleh agensi CISO.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
SI-4: Pemantauan Sistem (ditentukan IRS)	Semua titik Akses Internet/portal harus menangkap dan menyimpan, setidakny a selama satu tahun, informasi header lalu lintas masuk dan keluar, dengan pengecualian koneksi Internet “anonim” yang disetujui, sebagaimana dapat disetujui oleh agensi CISO.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilk an tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4: Pemantauan Sistem (ditentukan IRS)	Semua titik Akses Internet/portal harus menangkap dan menyimpan, setidakny a selama satu tahun, informasi header lalu lintas masuk dan keluar, dengan pengecualian koneksi Internet “anonim” yang disetujui, sebagaimana dapat disetujui oleh agensi CISO.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
SI-4: Pemantauan Sistem (ditentukan IRS)	Semua titik Akses Internet/portal harus menangkap dan menyimpan, setidakny a selama satu tahun, informasi header lalu lintas masuk dan keluar, dengan pengecualian koneksi Internet “anonim” yang disetujui, sebagaimana dapat disetujui oleh agensi CISO.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4: Pemantauan Sistem (ditentukan IRS)	Semua titik Akses Internet/portal harus menangkap dan menyimpan, setidakny a selama satu tahun, informasi header lalu lintas masuk dan keluar, dengan pengecualian koneksi Internet “anonim” yang disetujui, sebagaimana dapat disetujui oleh agensi CISO.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4: Pemantauan Sistem (ditentukan IRS)	Semua titik Akses Internet/portal harus menangkap dan menyimpan, setidaknya selama satu tahun, informasi header lalu lintas masuk dan keluar, dengan pengecualian koneksi Internet “anonim” yang disetujui, sebagaimana dapat disetujui oleh agensi CISO.	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7: Perangkat Lunak, Firmware, dan Integritas Informasi	Gunakan alat verifikasi integritas untuk mendeteksi perubahan yang tidak sah pada perangkat lunak, firmware, dan informasi berikut: kernel sistem, driver, firmware (misalnya , BIOS, UEFI), perangkat lunak (misalnya, OS, aplikasi, middleware) dan atribut keamanan.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7: Perangkat Lunak, Firmware, dan Integritas Informasi	Gunakan alat verifikasi integritas untuk mendeteksi perubahan yang tidak sah pada perangkat lunak, firmware, dan informasi berikut: kernel sistem, driver, firmware (misalnya , BIOS, UEFI), perangkat lunak (misalnya, OS, aplikasi, middleware) dan atribut keamanan.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7: Perangkat Lunak, Firmware, dan Integritas Informasi	Gunakan alat verifikasi integritas untuk mendeteksi perubahan yang tidak sah pada perangkat lunak, firmware, dan informasi berikut: kernel sistem, driver, firmware (misalnya , BIOS, UEFI), perangkat lunak (misalnya, OS, aplikasi, middleware) dan atribut keamanan.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12: Manajemen dan Retensi Informasi	Mengelola dan menyimpan informasi dalam sistem dan output informasi dari sistem sesuai dengan hukum yang berlaku, perintah eksekutif, arahan, peraturan, kebijakan , standar, pedoman, dan persyaratan operasional.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12: Manajemen dan Retensi Informasi	Mengelola dan menyimpan informasi dalam sistem dan output informasi dari sistem sesuai dengan hukum yang berlaku, perintah eksekutif, arahan, peraturan, kebijakan, standar, pedoman, dan persyaratan operasional.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12: Manajemen dan Retensi Informasi	Mengelola dan menyimpan informasi dalam sistem dan output informasi dari sistem sesuai dengan hukum yang berlaku, perintah eksekutif, arahan, peraturan, kebijakan, standar, pedoman, dan persyaratan operasional.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12: Manajemen dan Retensi Informasi	Mengelola dan menyimpan informasi dalam sistem dan output informasi dari sistem sesuai dengan hukum yang berlaku, perintah eksekutif, arahan, peraturan, kebijakan, standar, pedoman, dan persyaratan operasional.	dynamodb-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12: Manajemen dan Retensi Informasi	Mengelola dan menyimpan informasi dalam sistem dan output informasi dari sistem sesuai dengan hukum yang berlaku, perintah eksekutif, arahan, peraturan, kebijakan , standar, pedoman, dan persyaratan operasional.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12: Manajemen dan Retensi Informasi	Mengelola dan menyimpan informasi dalam sistem dan output informasi dari sistem sesuai dengan hukum yang berlaku, perintah eksekutif, arahan, peraturan, kebijakan, standar, pedoman, dan persyaratan operasional.	ebs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Block Store (Amazon EBS) Anda adalah bagian dari paket Cadangan. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12: Manajemen dan Retensi Informasi	Mengelola dan menyimpan informasi dalam sistem dan output informasi dari sistem sesuai dengan hukum yang berlaku, perintah eksekutif, arahan, peraturan, kebijakan, standar, pedoman, dan persyaratan operasional.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12: Manajemen dan Retensi Informasi	Mengelola dan menyimpan informasi dalam sistem dan output informasi dari sistem sesuai dengan hukum yang berlaku, perintah eksekutif, arahan, peraturan, kebijakan, standar, pedoman, dan persyaratan operasional.	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12: Manajemen dan Retensi Informasi	Mengelola dan menyimpan informasi dalam sistem dan output informasi dari sistem sesuai dengan hukum yang berlaku, perintah eksekutif, arahan, peraturan, kebijakan, standar, pedoman, dan persyaratan operasional.	efs-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12: Manajemen dan Retensi Informasi	Mengelola dan menyimpan informasi dalam sistem dan output informasi dari sistem sesuai dengan hukum yang berlaku, perintah eksekutif, arahan, peraturan, kebijakan , standar, pedoman, dan persyaratan operasional.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12: Manajemen dan Retensi Informasi	Mengelola dan menyimpan informasi dalam sistem dan output informasi dari sistem sesuai dengan hukum yang berlaku, perintah eksekutif, arahan, peraturan, kebijakan, standar, pedoman, dan persyaratan operasional.	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12: Manajemen dan Retensi Informasi	Mengelola dan menyimpan informasi dalam sistem dan output informasi dari sistem sesuai dengan hukum yang berlaku, perintah eksekutif, arahan, peraturan, kebijakan, standar, pedoman, dan persyaratan operasional.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relational Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12: Manajemen dan Retensi Informasi	Mengelola dan menyimpan informasi dalam sistem dan output informasi dari sistem sesuai dengan hukum yang berlaku, perintah eksekutif, arahan, peraturan, kebijakan, standar, pedoman, dan persyaratan operasional.	rds-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Relational Database Service (Amazon RDS) Anda merupakan AWS bagian dari paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12: Manajemen dan Retensi Informasi	Mengelola dan menyimpan informasi dalam sistem dan output informasi dari sistem sesuai dengan hukum yang berlaku, perintah eksekutif, arahan, peraturan, kebijakan, standar, pedoman, dan persyaratan operasional.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12: Manajemen dan Retensi Informasi	Mengelola dan menyimpan informasi dalam sistem dan output informasi dari sistem sesuai dengan hukum yang berlaku, perintah eksekutif, arahan, peraturan, kebijakan, standar, pedoman, dan persyaratan operasional.	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12: Manajemen dan Retensi Informasi	Mengelola dan menyimpan informasi dalam sistem dan output informasi dari sistem sesuai dengan hukum yang berlaku, perintah eksekutif, arahan, peraturan, kebijakan, standar, pedoman, dan persyaratan operasional.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12: Manajemen dan Retensi Informasi	Mengelola dan menyimpan informasi dalam sistem dan output informasi dari sistem sesuai dengan hukum yang berlaku, perintah eksekutif, arahan, peraturan, kebijakan, standar, pedoman, dan persyaratan operasional.	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12: Manajemen dan Retensi Informasi	Mengelola dan menyimpan informasi dalam sistem dan output informasi dari sistem sesuai dengan hukum yang berlaku, perintah eksekutif, arahan, peraturan, kebijakan, standar, pedoman, dan persyaratan operasional.	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12: Manajemen dan Retensi Informasi	Mengelola dan menyimpan informasi dalam sistem dan output informasi dari sistem sesuai dengan hukum yang berlaku, perintah eksekutif, arahan, peraturan, kebijakan, standar, pedoman, dan persyaratan operasional.	s3- lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihkan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).
SI-12: Manajemen dan Retensi Informasi	Mengelola dan menyimpan informasi dalam sistem dan output informasi dari sistem sesuai dengan hukum yang berlaku, perintah eksekutif, arahan, peraturan, kebijakan, standar, pedoman, dan persyaratan operasional.	s3- version-lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihkan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12: Manajemen dan Retensi Informasi	Mengelola dan menyimpan informasi dalam sistem dan output informasi dari sistem sesuai dengan hukum yang berlaku, perintah eksekutif, arahan, peraturan, kebijakan , standar, pedoman, dan persyaratan operasional.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12: Manajemen dan Retensi Informasi	Mengelola dan menyimpan informasi dalam sistem dan output informasi dari sistem sesuai dengan hukum yang berlaku, perintah eksekutif, arahan, peraturan, kebijakan , standar, pedoman, dan persyaratan operasional.	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk IRS 1075.

Praktik Terbaik Operasional untuk K-ISMS

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara Korea — Sistem Manajemen Keamanan Informasi (ISMS) dan aturan Config AWS terkelola. Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan berhubungan dengan satu atau lebih Korea - kontrol ISMS. Kontrol Korea - ISMS dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	AWS Aturan Config	Bimbingan
1.2.1	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigura si ke instans terkelola Anda dan memungkinkan Anda untuk menetapkan garis dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.
1.2.1	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirk an ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.
2.1.3	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager

ID Kontrol	AWS Aturan Config	Bimbingan
		menetapkan status konfigura si ke instans terkelola Anda dan memungkinkan Anda untuk menetapkan garis dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.
2.1.3	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirk an ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.
2.3.3	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatc h untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaa n AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	AWS Aturan Config	Bimbingan
2.3.3	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penol akan dengan merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilka n, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
2.5.1	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaima na ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.5.1	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribus i kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertah ankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	AWS Aturan Config	Bimbingan
2.5.1	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabun gkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandun g tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkin kan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda

ID Kontrol	AWS Aturan Config	Bimbingan
2.5.1	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
2.5.1	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizink an tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi, pengembalian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedAc tionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.5.1	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
2.5.1	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
2.5.1	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.
2.5.1	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredensyal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
2.5.1	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurang i peluang bagi identitas untuk menerima atau mempertah ankan hak istimewa yang berlebihan.
2.5.1	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentif ikasi, Anda harus menonakti fkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.5.1	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensyal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
2.5.1	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifka n untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensyal masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
2.5.1	secretsmanager-using-cmk	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
2.5.3	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredensyal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
2.5.3	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensyal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
2.5.3	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifka n untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensyal masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
2.5.4	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
2.5.5	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.
2.5.5	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	AWS Aturan Config	Bimbingan
2.5.5	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensyal masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
2.6	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.6	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.
2.6	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
2.6	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
2.6	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredensyal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
2.6	dibatasi ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.
2.6	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	AWS Aturan Config	Bimbingan
2.6	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyarat an untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	AWS Aturan Config	Bimbingan
2.6	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensyal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
2.6	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
2.6	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
2.6	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
2.6	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,338 9,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
2.6	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifka n untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensyal masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
2.6	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
2.6	s3- bucket-public-read-prohibit ed	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	AWS Aturan Config	Bimbingan
2.6	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
2.6	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
2.6	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .
2.6	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	AWS Aturan Config	Bimbingan
2.6.6	api-gw-associated-with-waf	AWS WAF memungkin kan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindung inya dari serangan berbahaya
2.6.6	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan membantu melindung i data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
2.6.6	lambda-function-public-acce ss-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses publik. Akses publik berpotens i menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	AWS Aturan Config	Bimbingan
2.6.6	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
2.6.6	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
2.6.6	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,338 9,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.6.6	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
2.6.6	s3- bucket-public-read-prohibit ed	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	AWS Aturan Config	Bimbingan
2.6.6	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
2.6.6	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
2.6.6	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .
2.6.6	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	AWS Aturan Config	Bimbingan
2.6.7	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
2.7	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastika n sertifikat X509 dikeluark an oleh AWS ACM. Sertifika t ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
2.7	alb-http-drop-invalid-Header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhk an header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
2.7	alb-http-to-https-pengalihan-periksa	Untuk membantu melindung i data dalam perjalanan, pastikan bahwa Applicati on Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
2.7	api-gw-cache-enabled-dan-di enkripsi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
2.7	cloudwatch-log-group-encryp ted	Untuk membantu melindung i data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
2.7	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.7	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
2.7	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
2.7	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.7	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
2.7	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
2.7	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindung i data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	AWS Aturan Config	Bimbingan
2.7	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
2.7	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
2.7	rds-snapshot-encrypted	Pastikan enkripsi diaktifka n untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
2.7	rds-storage-encrypted	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
2.7	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastika n bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberika n informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.7	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
2.7	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
2.7	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
2.7	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
2.7	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
2.7	sns-encrypted-kms	Untuk membantu melindung i data saat istirahat, pastikan topik Amazon Simple Notificat ion Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
2.7	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
2.7	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
2.7.1	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifika t SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.

ID Kontrol	AWS Aturan Config	Bimbingan
2.7.1	elb-predefined-security-policy-ssl-periksa	Untuk membantu melindung i data dalam perjalanan, pastikan bahwa pendengar SSL Classic Elastic Load Balancing Anda menggunak an kebijakan keamanan yang telah ditentukan sebelumny a. Elastic Load Balancing menyediakan konfigurasi negosiasi SSL yang telah ditentukan sebelumny a yang digunakan untuk negosiasi SSL ketika koneksi dibuat antara klien dan penyeimbang beban Anda. Konfigurasi negosiasi SSL memberikan kompatibilitas dengan berbagai klien dan menggunakan algoritma kriptografi berkekuatan tinggi. Aturan ini mengharus kan Anda menetapkan kebijakan keamanan yang telah ditentukan untuk pendengar SSL Anda. Kebijakan keamanan default adalah: ELBSecurity Policy-TLS-1-2-2017-0. Nilai aktual harus mencerminkan kebijakan organisasi Anda

ID Kontrol	AWS Aturan Config	Bimbingan
2.7.2	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.
2.7.2	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.
2.8.5	codebuild-project-envvar-awscred-periksa	Pastikan kredensyal otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild. Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
2.8.5	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredensyal masuk dalam lingkungan proyek Codebuild. AWS Gunakan OAuth alih-alih token akses pribadi atau kredensyal masuk untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.
2.8.6	codebuild-project-envvar-awscred-periksa	Pastikan kredensyal otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild. Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
2.8.6	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredensyal masuk dalam lingkungan proyek Codebuild. AWS Gunakan OAuth alih-alih token akses pribadi atau kredensyal masuk untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.
2.9.1	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizat ions membantu memastika n bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabk an konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.
2.9.1	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktif an beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	AWS Aturan Config	Bimbingan
2.9.1	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	AWS Aturan Config	Bimbingan
2.9.1	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.9.2	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	AWS Aturan Config	Bimbingan
2.9.2	cloudwatch-alarm-action-check	Amazon CloudWatch memperingatkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.9.2	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.9.2	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.
2.9.2	lambda-concurrency-check	Aturan ini memastikan bahwa batas tinggi dan rendah konkurensi fungsi Lambda ditetapkan. Ini dapat membantu dalam mendasark an jumlah permintaan yang dilayani oleh fungsi Anda pada waktu tertentu.

ID Kontrol	AWS Aturan Config	Bimbingan
2.9.2	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.
2.9.3	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.9.3	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.
2.9.3	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.9.3	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
2.9.3	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.9.3	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.
2.9.3	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	AWS Aturan Config	Bimbingan
2.9.3	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
2.9.3	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.9.3	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relational Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.9.3	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independe n yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
2.9.3	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.
2.9.3	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersedi aan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	AWS Aturan Config	Bimbingan
2.9.3	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihka n setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	AWS Aturan Config	Bimbingan
2.9.3	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimpleme ntasikan untuk mencapai persyaratan ketahanan . Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-S ite VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	AWS Aturan Config	Bimbingan
2.9.3	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
2.9.3	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.9.4	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
2.9.4	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
2.9.4	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	AWS Aturan Config	Bimbingan
2.9.4	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penol akan dengan merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilka n, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
2.9.4	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	AWS Aturan Config	Bimbingan
2.9.4	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifka n. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	AWS Aturan Config	Bimbingan
2.9.4	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimk an file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
2.9.4	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
2.9.4	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	AWS Aturan Config	Bimbingan
2.9.4	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
2.9.4	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	AWS Aturan Config	Bimbingan
2.10.3	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirk an ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.
2.10.3	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.10.3	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan: rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.10.3	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigura si ke instans terkelola Anda dan memungkinkan Anda untuk menetapkan garis dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.
2.10.3	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan , sesuai dengan standar organisasi Anda.
2.10.5	alb-http-drop-invalid-Header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhk an header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
2.10.5	alb-http-to-https-pengalihan-periksa	Untuk membantu melindung i data dalam perjalanan, pastikan bahwa Applicati on Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
2.10.5	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
2.10.5	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindung i data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
2.10.5	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
2.10.5	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerluka n enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
2.10.5	s3- bucket-ssl-requests-only	Untuk membantu melindung i data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerluka n permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
2.10.5	opensearch-node-to-node- pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
2.10.8	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigura si ke instans terkelola Anda dan memungkinkan Anda untuk menetapkan garis dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.
2.10.8	ec2- -periksa managedin stance-patch-compliance-sta tus	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.11.2	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan: rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.11.3	cloudwatch-alarm-action-check	Amazon CloudWatch memperingatkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.
2.11.3	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	AWS Aturan Config	Bimbingan
2.11.3	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
2.11.3	lambda-concurrency-check	Aturan ini memastikan bahwa batas tinggi dan rendah konkurensi fungsi Lambda ditetapkan. Ini dapat membantu dalam mendasark an jumlah permintaan yang dilayani oleh fungsi Anda pada waktu tertentu.

ID Kontrol	AWS Aturan Config	Bimbingan
2.11.3	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	AWS Aturan Config	Bimbingan
2.11.3	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
2.12	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.12	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.
2.12	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.12	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
2.12	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.12	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.
2.12	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	AWS Aturan Config	Bimbingan
2.12	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
2.12	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.12	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relational Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.12	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independe n yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
2.12	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk cluster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.
2.12	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
2.12	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersedi aan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.
2.12	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihka n setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	AWS Aturan Config	Bimbingan
2.12	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimpleme ntasikan untuk mencapai persyaratan ketahanan . Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-S ite VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	AWS Aturan Config	Bimbingan
2.12	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.12	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk K-ISMS.

Praktik Terbaik Operasional untuk Load Balancing

Paket kesesuaian ini berisi AWS Config aturan berdasarkan load balancing di dalamnya. AWS Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Penyeimbangan Beban.

Praktik Terbaik Operasional untuk Penebangan

Paket kesesuaian ini berisi AWS Config aturan berdasarkan pencatatan di dalamnya. AWS Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Logging.

Praktik Terbaik Operasional untuk Layanan Manajemen dan Tata Kelola

Paket kesesuaian ini berisi AWS Config aturan berdasarkan Layanan Manajemen dan Tata Kelola. Untuk informasi selengkapnya, lihat Manajemen dan Tata Kelola di AWS. Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template ini tersedia di GitHub: Praktik Terbaik Operasional untuk Layanan Manajemen dan Tata Kelola.

Praktik Terbaik Operasional untuk Pemberitahuan MAS 655

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara Pemberitahuan Otoritas Moneter Singapura (MAS) 655 — Cyber Hygiene dan aturan AWS Config yang dikelola. Setiap aturan Config berlaku

untuk AWS sumber daya tertentu, dan terkait dengan satu atau lebih Pemberitahuan MAS 655 — kontrol Cyber Hygiene. Pemberitahuan MAS 655 — Kontrol Cyber Hygiene dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	AWS Aturan Config	Bimbingan
4.1	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurang i peluang bagi identitas untuk menerima atau mempertah ankan hak istimewa yang berlebihan.
4.1	access-keys-rotated	Kredensi diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaima na ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus

ID Kontrol	AWS Aturan Config	Bimbingan
		mencerminkan kebijakan organisasi Anda.
4.1	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentif ikasi, Anda harus menonakti fkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
4.1	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
4.1	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifka n untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensyal masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
4.1	ec2- instance-profile-attached	EC2 profil instance meneruska n peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
4.1	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabun gkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandun g tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkin kan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda

ID Kontrol	AWS Aturan Config	Bimbingan
4.1	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizink an tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi, pengembalian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedAc tionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
4.1	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.
4.1	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensyal masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
4.1	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensyal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
4.1	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredensyal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
4.1	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribus i kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertah ankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	AWS Aturan Config	Bimbingan
4.1	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.
4.1	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
4.1	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.
4.1	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabun gkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
4.1	secretsmanager-rotation-enabled-check	Aturan ini memastikan AWS rahasia Secrets Manager telah diaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikomprom ikan.
4.1	secretsmanager-scheduled-rotation-success-periksa	Aturan ini memastikan bahwa AWS rahasia Secrets Manager telah berhasil diputar sesuai dengan jadwal rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode di mana rahasia aktif, dan berpotensi mengurangi dampak bisnis jika dikomprom ikan.
4.1	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
4.2	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.
4.2	ec2- -periksa managedin stance-patch-compliance-sta tus	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
4.2	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapka n status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigura si aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
4.2	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
4.2	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunak an kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.
4.2	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	AWS Aturan Config	Bimbingan
4.2	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relationa l Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.
4.2	ecr-private-image-scanning-diaktifkan	Pemindaian gambar Amazon Elastic Container Repository (ECR) membantu mengident ifikasi kerentanan perangkat lunak dalam gambar kontainer Anda. Mengaktif kan pemindaian gambar pada repositori ECR menambahk an lapisan verifikasi untuk integritas dan keamanan gambar yang disimpan.

ID Kontrol	AWS Aturan Config	Bimbingan
4.3	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.
4.3	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	AWS Aturan Config	Bimbingan
4.3	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapka n status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigura si aplikasi, dan detail lainnya tentang lingkungan Anda.
4.3	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizat ions membantu memastika n bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabk an konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.

ID Kontrol	AWS Aturan Config	Bimbingan
4.4	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.
4.4	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
4.4	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
4.4	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
4.4	ec2- security-group-attached-to -eni-periodik	Aturan ini memastikan grup keamanan dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) atau ke ENI. Aturan ini membantu memantau kelompok keamanan yang tidak digunakan dalam inventaris dan pengelolaan lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
4.4	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearc h Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
4.4	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
4.4	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
4.4	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	AWS Aturan Config	Bimbingan
4.4	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	AWS Aturan Config	Bimbingan
4.4	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkin kan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabk an akses tidak sah ke sumber daya VPC Amazon.
4.4	lambda-function-public-acce ss-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	AWS Aturan Config	Bimbingan
4.4	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyarat an untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.
4.4	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
4.4	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
4.4	waf-regional-rule-not-kosong	Pastikan AWS WAF Anda memiliki aturan yang tidak kosong. Aturan tanpa kondisi dapat mengakibatkan perilaku yang tidak diinginkan.
4.4	waf-regional-rulegroup-not-kosong	Pastikan AWS WAF Anda memiliki grup aturan yang tidak kosong. Grup aturan yang kosong dapat mengakibatkan perilaku yang tidak diinginkan.
4.4	waf-regional-webacl-not-kosong	Web ACL yang dilampirkan ke AWS WAF dapat berisi kumpulan aturan dan kelompok aturan untuk memeriksa dan mengontrol permintaan web. Jika ACL Web kosong, lalu lintas web lewat tanpa terdeteksi atau ditindaklanjuti oleh WAF.

ID Kontrol	AWS Aturan Config	Bimbingan
4.4	netfw-policy-default-action-fragmen-paket	Kebijakan AWS Network Firewall mendefinisikan bagaimana firewall Anda memantau dan menangani lalu lintas di VPC Amazon. Anda mengonfigurasi grup aturan stateless dan stateful untuk memfilter paket dan arus lalu lintas. Default ke tindakan Pass dapat memungkinkan lalu lintas yang tidak diinginkan.
4.4	netfw-policy-default-action-paket penuh	Kebijakan AWS Network Firewall mendefinisikan bagaimana firewall Anda memantau dan menangani lalu lintas di VPC Amazon. Anda mengonfigurasi grup aturan stateless dan stateful untuk memfilter paket dan arus lalu lintas. Default ke tindakan Pass dapat memungkinkan lalu lintas yang tidak diinginkan.

ID Kontrol	AWS Aturan Config	Bimbingan
4.4	netfw-policy-rule-group-terkait	Kebijakan AWS Network Firewall mendefinisikan bagaimana firewall Anda memantau dan menangani lalu lintas di VPC Amazon. Anda mengonfigurasi grup aturan stateless dan stateful untuk memfilter paket dan arus lalu lintas, dan Anda menentukan penanganan lalu lintas default.
4.4	netfw-stateless-rule-group-tidak-kosong	Grup aturan AWS Network Firewall berisi aturan yang menentukan bagaimana firewall Anda memproses lalu lintas di VPC Anda. Grup aturan stateless kosong saat ada dalam kebijakan firewall tidak memproses lalu lintas.
4.4	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
4.4	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,338 9,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
4.4	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
4.4	sagemaker-notebook-no-direc t-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
4.4	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .
4.4	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam grup keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	AWS Aturan Config	Bimbingan
4.4	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
4.4	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
4.4	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
4.4	s3- -dilarang bucket-level-publi c-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
4.4	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	AWS Aturan Config	Bimbingan
4.4	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
4.4	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositori data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	AWS Aturan Config	Bimbingan
4.4	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspo s informasi tentang akun, sumber daya, dan proses internal Anda.
4.4	api-gw-associated-with-waf	AWS WAF memungkin kan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindung inya dari serangan berbahaya

ID Kontrol	AWS Aturan Config	Bimbingan
4.4	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearc h Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
4.5	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
4.5	ec2- -periksa managedin stance-patch-compliance-sta tus	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
4.5	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapka n status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigura si aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
4.5	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
4.6	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
4.6	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifka n untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensyal masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
4.6	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	AWS Aturan Config	Bimbingan
4.6	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensyal masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
4.6	mfa-enabled-for-iam-aksekonsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensyal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
4.6	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredensyal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

Templat

Template ini tersedia di GitHub: Praktik Terbaik Operasional untuk Pemberitahuan MAS 655.

Praktik Terbaik Operasional untuk MAS TRMG

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara Pedoman Manajemen Risiko Teknologi Otoritas Moneter Singapura (MAS) (TRMG) Januari 2021 dan aturan Konfigurasi terkelola AWS . Setiap aturan AWS Config berlaku untuk AWS sumber daya tertentu, dan berhubungan dengan satu atau lebih kontrol MAS TRMG. Kontrol MAS TRMG Januari 2021 dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	AWS Aturan Config	Bimbingan
3.3.1	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizat ions membantu memastika n bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabk an konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.
5.4.3	codebuild-project-envvar-aw scred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_ KEY tidak ada dalam lingkungan proyek AWS Codebuild. Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabk an paparan data yang tidak diinginkan dan akses yang tidak sah.
5.4.3	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredenal masuk dalam lingkungan proyek Codebuild. AWS Gunakan OAuth alih-alih token akses pribadi atau kredensyal masuk untuk memberikan otorisasi

ID Kontrol	AWS Aturan Config	Bimbingan
		untuk mengakses GitHub atau repositori Bitbucket.
6.1.1	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild. Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.
6.1.2	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild. Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
6.1.4	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.
6.1.4	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapka n status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigura si aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
6.1.4	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
6.2.1	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.
6.3.1	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	AWS Aturan Config	Bimbingan
6.4.5	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
6.4.5	alb-http-to-https-pemeriksaan-pengalihan	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
6.4.5	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.

ID Kontrol	AWS Aturan Config	Bimbingan
6.4.5	cmk-backing-key-rotation-di aktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.
6.4.5	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
6.4.5	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
6.4.5	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindung i data dalam perjalanan, pastikan HTTPS diaktifka n untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
6.4.5	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindung i data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
6.4.5	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
6.4.5	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan membantu melindung i data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
6.4.5	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerluka n enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
6.4.5	s3- bucket-ssl-requests-only	Untuk membantu melindung i data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerluka n permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
6.4.6	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
6.4.6	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
6.4.6	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	AWS Aturan Config	Bimbingan
6.4.6	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.
6.4.6	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	AWS Aturan Config	Bimbingan
6.4.6	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimk an file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
6.4.6	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
6.4.6	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
6.4.6	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.
6.4.6	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkunga n Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberika n informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	AWS Aturan Config	Bimbingan
6.4.7	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
6.4.7	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
6.4.7	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	AWS Aturan Config	Bimbingan
6.4.7	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.
6.4.7	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	AWS Aturan Config	Bimbingan
6.4.7	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktif an beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.
6.4.7	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	AWS Aturan Config	Bimbingan
6.4.7	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifka n. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.
6.4.7	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
6.4.7	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimk an file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
6.4.7	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
6.4.7	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
6.4.7	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	AWS Aturan Config	Bimbingan
6.4.7	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
6.4.7	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkunga n Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberika n informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	AWS Aturan Config	Bimbingan
6.4.8	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuai kan kapasitas throughpu t yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/ tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.
6.4.8	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersedi aan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	AWS Aturan Config	Bimbingan
6.4.8	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.
6.4.8	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	AWS Aturan Config	Bimbingan
6.4.8	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
6.4.8	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
6.4.8	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independe n yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
6.4.8	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimpleme ntasikan untuk mencapai persyaratan ketahanan . Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-S ite VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	AWS Aturan Config	Bimbingan
7.2.1	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.
7.2.1	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapka n status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigura si aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
7.4.1	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.
7.4.1	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapka n status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigura si aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
7.4.1	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
7.4.1	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	AWS Aturan Config	Bimbingan
7.4.1	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relationa l Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.

ID Kontrol	AWS Aturan Config	Bimbingan
7.4.1	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
7.5.5	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.
7.5.5	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
7.5.5	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan cadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.
7.5.5	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
7.5.5	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
7.5.5	elasticache-redis-cluster-a utomatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCac he membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentuka n oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	AWS Aturan Config	Bimbingan
7.5.5	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relational Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
7.5.5	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	AWS Aturan Config	Bimbingan
7.5.5	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersedi aan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.
7.5.5	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihka n setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	AWS Aturan Config	Bimbingan
7.5.7	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
7.5.7	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
7.5.7	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	AWS Aturan Config	Bimbingan
7.5.7	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
7.5.7	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
7.5.7	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
7.5.7	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
7.5.7	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	AWS Aturan Config	Bimbingan
7.5.7	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
7.5.7	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.
7.5.7	vpc-flow-logs-enabled	Log aliran VPC menyediak an catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	AWS Aturan Config	Bimbingan
7.5.7	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
8.1.1	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	AWS Aturan Config	Bimbingan
8.1.1	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.
8.1.1	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	AWS Aturan Config	Bimbingan
8.1.1	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.
8.1.1	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
8.1.1	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
8.1.1	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independe n yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
8.1.1	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimpleme ntasikan untuk mencapai persyaratan ketahanan . Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-S ite VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	AWS Aturan Config	Bimbingan
8.1.2	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	AWS Aturan Config	Bimbingan
8.1.2	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independe n yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
8.1.2	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersedi aan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.
8.1.2	opensearch-data-node-fault-toleransi	Amazon OpenSearch Service (OpenSearch Service) memerlukan setidaknya tiga node data untuk ketersedi aan tinggi dan toleransi kesalahan. Menyebarkan domain OpenSearch Service dengan setidaknya tiga node data memastikan operasi cluster jika node gagal.

ID Kontrol	AWS Aturan Config	Bimbingan
8.1.2	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.
8.1.3	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	AWS Aturan Config	Bimbingan
8.1.3	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.
8.1.3	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	AWS Aturan Config	Bimbingan
8.1.3	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penol akan dengan merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilka n, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
8.4.1	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
8.4.1	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
8.4.1	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan cadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	AWS Aturan Config	Bimbingan
8.4.1	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
8.4.1	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediak an kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
8.4.1	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
8.4.1	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relational Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
8.4.1	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.
8.4.1	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	AWS Aturan Config	Bimbingan
8.4.1	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersedi aan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.
8.4.1	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihka n setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	AWS Aturan Config	Bimbingan
8.4.2	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.
8.4.2	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
8.4.2	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan cadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.
8.4.2	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
8.4.2	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.
8.4.2	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
8.4.2	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.
8.4.2	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relational Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
8.4.2	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.
8.4.2	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersedi aan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	AWS Aturan Config	Bimbingan
8.4.2	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihka n setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.
8.4.4	rds-snapshot-encrypted	Pastikan enkripsi diaktifka n untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
8.5.4	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independe n yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	AWS Aturan Config	Bimbingan
8.5.4	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersedi aan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.
9.1.1	ec2- instance-profile-attached	EC2 profil instance meneruska n peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.
9.1.1	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.1	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribus i kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertah ankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.1	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabun gkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandun g tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkin kan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.1	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.1	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizink an tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi, pengembalian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedAc tionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.1	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.1	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
9.1.1	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
9.1.1	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.1	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.
9.1.1	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.1	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
9.1.1	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurang i peluang bagi identitas untuk menerima atau mempertah ankan hak istimewa yang berlebihan.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.1	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentif ikasi, Anda harus menonakti fkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.1	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
9.1.1	root-account-hardware-mfa-d iaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.1	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifka n untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
9.1.1	secretsmanager-rotation-ena bled-check	Aturan ini memastikan AWS rahasia Secrets Manager telah diaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotens i mengurangi dampak bisnis jika rahasia itu dikomprom ikan.
9.1.1	secretsmanager-scheduled-ro tation-success-periksa	Aturan ini memastikan bahwa AWS rahasia Secrets Manager telah berhasil diputar sesuai dengan jadwal rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode di mana rahasia aktif, dan berpotensi mengurangi dampak bisnis jika dikomprom ikan.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.1	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_ bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs
9.1.1	secretsmanager-secret-periodic-rotation	Aturan ini memastikan AWS rahasia Secrets Manager mengaktifkan rotasi periodik. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan. Nilai defaultnya adalah 90 hari.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.1	secretsmanager-secret-unused	Jika kredensil yang tidak digunakan ada di AWS Secrets Manager, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa terkecil. Aturan ini memungkinkan Anda untuk menetapkan nilai ke unusedForDays (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.2	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabun gkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandun g tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkin kan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.2	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.2	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizink an tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi, pengembalian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedAc tionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.2	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.2	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
9.1.2	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.3	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
9.1.3	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
9.1.3	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.3	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.
9.1.3	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.3	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktif an beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.
9.1.3	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.
9.1.3	elasticsearch-logs-to-cloud watch	Pastikan domain OpenSearc h Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.3	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
9.1.3	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.3	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.3	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimk an file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.3	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
9.1.3	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.3	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.3	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
9.1.3	vpc-flow-logs-enabled	Log aliran VPC menyediak an catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.3	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.4	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
9.1.5	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
9.1.5	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.5	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
9.1.5	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.6	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentif ikasi, Anda harus menonakti fkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.7	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribus i kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertah ankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.7	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabun gkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandun g tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkin kan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.7	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.7	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizink an tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi, pengembalian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedAc tionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.7	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	AWS Aturan Config	Bimbingan
9.1.7	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
9.2.1	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
9.2.1	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	AWS Aturan Config	Bimbingan
9.2.1	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkin kan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
9.2.1	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penol akan dengan merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilka n, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
9.2.1	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
9.2.1	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.
9.2.1	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	AWS Aturan Config	Bimbingan
9.2.1	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
9.2.1	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimk an file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
9.2.1	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
9.2.1	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
9.2.2	api-gw-execution-logging-di aktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
9.2.2	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatc h untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaa n AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	AWS Aturan Config	Bimbingan
9.2.2	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penol akan dengan merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilka n, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
9.2.2	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
9.2.2	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.
9.2.2	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	AWS Aturan Config	Bimbingan
9.2.2	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.
9.2.2	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
9.2.2	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimk an file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
9.2.2	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
9.2.2	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
9.3.1	alb-http-to-https-pemeriksaan-pengalihan	Untuk membantu melindung i data dalam perjalanan, pastikan bahwa Applicati on Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
9.3.1	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifika t SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
9.3.1	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
9.3.1	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
9.3.1	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.
9.3.1	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	AWS Aturan Config	Bimbingan
9.3.1	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.
9.3.1	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	AWS Aturan Config	Bimbingan
9.3.1	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
9.3.1	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentif ikasi, Anda harus menonakti fkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
9.3.1	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
9.3.1	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerluka n enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
9.3.1	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
9.3.1	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
9.3.1	s3- bucket-ssl-requests-only	Untuk membantu melindung i data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerluka n permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
10.1.1	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastika n sertifikat X509 dikeluark an oleh AWS ACM. Sertifika t ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
10.1.1	alb-http-to-https-pemeriksaan-pengalihan	Untuk membantu melindung i data dalam perjalanan, pastikan bahwa Applicati on Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
10.1.1	api-gw-cache-enabled-dan-di enkripsi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
10.1.1	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifika t SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	AWS Aturan Config	Bimbingan
10.1.1	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
10.1.1	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
10.1.1	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
10.1.1	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
10.1.1	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
10.1.1	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
10.1.1	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
10.1.1	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
10.1.1	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
10.1.1	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certifica te Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
10.1.1	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
10.1.1	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certifica te Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
10.1.1	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
10.1.1	rds-snapshot-encrypted	Pastikan enkripsi diaktifka n untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
10.1.1	rds-storage-encrypted	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
10.1.1	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastika n bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberika n informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
10.1.1	redshift-cluster-kms-enabled	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
10.1.1	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerluka n enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
10.1.1	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
10.1.1	s3- bucket-ssl-requests-only	Untuk membantu melindung i data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerluka n permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
10.1.1	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
10.1.1	sagemaker-endpoint-configur ation-kms-kunci-dikonfigurasi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
10.1.1	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
10.1.1	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
10.1.1	sns-encrypted-kms	Untuk membantu melindung i data saat istirahat, pastikan topik Amazon Simple Notificat ion Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
10.2.1	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastika n sertifikat X509 dikeluark an oleh AWS ACM. Sertifika t ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
10.2.1	cmk-backing-key-rotation-di aktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	AWS Aturan Config	Bimbingan
10.2.1	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.
10.2.2	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	AWS Aturan Config	Bimbingan
10.2.3	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaima na ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
10.2.3	cmk-backing-key-rotation-di aktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	AWS Aturan Config	Bimbingan
10.2.3	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.
11.1.1 (a)	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.1 (a)	alb-http-to-https-pemeriksaan-pengalihan	Untuk membantu melindung i data dalam perjalanan, pastikan bahwa Applicati on Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
11.1.1 (a)	api-gw-cache-enabled-dan-di enkripsi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
11.1.1 (a)	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifika t SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.1 (a)	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
11.1.1 (a)	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.1 (a)	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certifica te Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
11.1.1 (a)	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
11.1.1 (a)	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerluka n enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.1 (a)	s3- bucket-ssl-requests-only	Untuk membantu melindung i data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerluka n permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
11.1.1 (b)	api-gw-cache-enabled-dan-di enkripsi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
11.1.1 (b)	autoscaling-launch-config-p ublic-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.1 (b)	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
11.1.1 (b)	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
11.1.1 (b)	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
11.1.1 (b)	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.1 (b)	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
11.1.1 (b)	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
11.1.1 (b)	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.1 (b)	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
11.1.1 (b)	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
11.1.1 (b)	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.1 (b)	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearc h Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
11.1.1 (b)	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearc h Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.1 (b)	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
11.1.1 (b)	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
11.1.1 (b)	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.1 (b)	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.
11.1.1 (b)	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.1 (b)	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyarat an untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.
11.1.1 (b)	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.1 (b)	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
11.1.1 (b)	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
11.1.1 (b)	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.1 (b)	rds-storage-encrypted	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
11.1.1 (b)	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastika n bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberika n informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.1 (b)	redshift-cluster-kms-enabled	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
11.1.1 (b)	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.1 (b)	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,338 9,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.1 (b)	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
11.1.1 (b)	s3- bucket-public-read-prohibit ed	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.1 (b)	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
11.1.1 (b)	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
11.1.1 (b)	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.1 (b)	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
11.1.1 (b)	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
11.1.1 (b)	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.1 (b)	secretsmanager-using-cmk	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
11.1.1 (b)	sns-encrypted-kms	Untuk membantu melindung i data saat istirahat, pastikan topik Amazon Simple Notificat ion Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.1 (b)	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspo s informasi tentang akun, sumber daya, dan proses internal Anda.
11.1.1 (b)	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.3	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
11.1.3	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
11.1.3	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
11.1.3	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.3	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
11.1.3	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
11.1.3	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.3	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.
11.1.3	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
11.1.3	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
11.1.3	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.3	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribus i kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertah ankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.3	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabun gkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandun g tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkin kan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.3	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.3	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizink an tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi, pengembalian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedAc tionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.3	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.3	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
11.1.3	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
11.1.3	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.3	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.
11.1.3	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.3	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurang i peluang bagi identitas untuk menerima atau mempertah ankan hak istimewa yang berlebihan.
11.1.3	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentif ikasi, Anda harus menonakti fkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.3	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
11.1.3	rds-snapshot-encrypted	Pastikan enkripsi diaktifka n untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.3	rds-storage-encrypted	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
11.1.3	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastika n bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberika n informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.3	redshift-cluster-kms-enabled	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
11.1.3	root-account-hardware-mfa-d iaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.3	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifka n untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
11.1.3	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
11.1.3	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.3	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
11.1.3	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
11.1.3	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
11.1.3	sns-encrypted-kms	Untuk membantu melindung i data saat istirahat, pastikan topik Amazon Simple Notificat ion Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
11.2.1	alb-waf-enabled	Pastikan AWS WAF diaktifka n pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
11.2.2	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
11.2.2	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
11.2.2	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
11.2.2	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
11.2.2	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearc h Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	AWS Aturan Config	Bimbingan
11.2.2	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearc h Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
11.2.2	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
11.2.2	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
11.2.2	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	AWS Aturan Config	Bimbingan
11.2.2	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.
11.2.2	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	AWS Aturan Config	Bimbingan
11.2.2	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyarat an untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.
11.2.2	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
11.2.2	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
11.2.2	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
11.2.2	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,338 9,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
11.2.2	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
11.2.2	s3- bucket-public-read-prohibit ed	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	AWS Aturan Config	Bimbingan
11.2.2	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
11.2.2	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
11.2.2	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	AWS Aturan Config	Bimbingan
11.2.2	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .
11.2.2	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	AWS Aturan Config	Bimbingan
11.2.4	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
11.2.4	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
11.2.4	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
11.2.4	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
11.2.4	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
11.2.4	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	AWS Aturan Config	Bimbingan
11.2.4	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	AWS Aturan Config	Bimbingan
11.2.4	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
11.2.4	api-gw-associated-with-waf	AWS WAF memungkin kan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindung inya dari serangan berbahaya

ID Kontrol	AWS Aturan Config	Bimbingan
11.2.4	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.
11.2.4	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyarat an untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	AWS Aturan Config	Bimbingan
11.2.4	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
11.2.4	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
11.2.4	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
11.2.4	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,338 9,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
11.2.4	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
11.2.4	s3- bucket-public-write-prohibi ted	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	AWS Aturan Config	Bimbingan
11.2.4	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
11.2.4	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	AWS Aturan Config	Bimbingan
11.2.4	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .
11.2.4	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	AWS Aturan Config	Bimbingan
11.3.1	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunak an kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.
11.3.5	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penol akan dengan merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilka n, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	AWS Aturan Config	Bimbingan
11.3.5	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
11.3.5	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimk an file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
11.3.5	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
11.4.2	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	AWS Aturan Config	Bimbingan
11.4.2	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,338 9,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
11.4.2	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	AWS Aturan Config	Bimbingan
11.4.2	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	AWS Aturan Config	Bimbingan
11.5.2	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
12.1.1	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penol akan dengan merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilka n, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	AWS Aturan Config	Bimbingan
12.1.1	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
12.1.1	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimk an file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
12.1.1	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
12.2.2	api-gw-execution-logging-di aktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
12.2.2	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatc h untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaa n AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	AWS Aturan Config	Bimbingan
12.2.2	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
12.2.2	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.
12.2.2	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	AWS Aturan Config	Bimbingan
12.2.2	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
12.2.2	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.
12.2.2	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	AWS Aturan Config	Bimbingan
12.2.2	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
12.2.2	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimk an file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
12.2.2	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
12.2.2	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
12.2.2	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	AWS Aturan Config	Bimbingan
12.2.2	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
12.2.2	vpc-flow-logs-enabled	Log aliran VPC menyediak an catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	AWS Aturan Config	Bimbingan
12.2.2	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
12.2.4	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
12.2.4	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
12.2.5	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penol akan dengan merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilka n, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	AWS Aturan Config	Bimbingan
12.2.5	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
12.2.5	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimk an file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
12.2.5	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
12.3.2	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
12.3.2	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimk an file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
12.3.2	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
14.1.2	alb-http-to-https-pemeriksaan-pengalihan	Untuk membantu melindung i data dalam perjalanan, pastikan bahwa Applicati on Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
14.1.2	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifika t SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
14.1.2	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
14.1.2	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
14.1.2	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certifica te Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
14.1.2	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
14.1.2	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certifica te Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	AWS Aturan Config	Bimbingan
14.1.2	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
14.1.2	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
14.1.3	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
14.1.3	api-gw-associated-with-waf	AWS WAF memungkin kan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindung inya dari serangan berbahaya
14.1.3	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengident ifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
14.1.3	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
14.2.2	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastika n sertifikat X509 dikeluark an oleh AWS ACM. Sertifika t ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
14.2.2	alb-http-to-https-pemeriksaan-pengalihan	Untuk membantu melindung i data dalam perjalanan, pastikan bahwa Applicati on Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
14.2.2	api-gw-cache-enabled-dan-di enkripsi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
14.2.2	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifika t SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	AWS Aturan Config	Bimbingan
14.2.2	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
14.2.2	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
14.2.2	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
14.2.2	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
14.2.2	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
14.2.2	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
14.2.2	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	AWS Aturan Config	Bimbingan
14.2.2	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
14.2.6	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	AWS Aturan Config	Bimbingan
14.2.6	ec2- ebs-encryption-by-default	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
14.2.6	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
14.2.6	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
14.2.6	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
14.2.6	rds-storage-encrypted	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
14.2.6	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
14.2.6	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk MAS TRMG.

Praktik Terbaik Operasional untuk Pemantauan

Paket kesesuaian ini berisi AWS Config aturan berdasarkan pemantauan di dalamnya. AWS Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Pemantauan.

Praktik Terbaik Operasional untuk NBC TRMG

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara kerangka Pedoman Manajemen Risiko Teknologi (TRM) Bank Nasional Kamboja (NBC) dan aturan Config yang dikelola. AWS Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau beberapa Pedoman NBC TRM. Pedoman TRM NBC dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

Contoh template paket kesesuaian ini berisi pemetaan ke kontrol dalam kerangka Pedoman Manajemen Risiko Teknologi (TRM) Bank Nasional Kamboja (NBC), yang dapat diakses di sini: Bank Nasional Kamboja: Pedoman Manajemen Risiko Teknologi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (d)	d) Di antara kontrol penting yang perlu dipertimb angkan adalah: - Proses sistemati s penerapan dan otorisasi pembuatan pengguna IDs dan matriks kontrol akses - Melakukan penilaian risiko dan pemberian hak akses berdasark an hal yang sama. - Implementasi kontrol akses berbasis peran yang dirancang	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	untuk memastika n pemisahan tugas yang efektif - Mengubah nama pengguna default and/or passwords of systems and prohibiti ng sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contrac t - Proses untuk memberi tahu secara tepat waktu fungsi keamanan informasi mengenai penambaha n, penghapusan, dan perubahan peran pengguna - Rekonsili asi berkala pengguna IDs dalam suatu sistem dan pengguna aktual diharuskan memiliki akses dan penghapusan yang tidak perlu IDs, jika ada - Audit, pencatata n, dan pemantaua n akses ke aset TI		menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	oleh semua pengguna dan - Mempertim bangkan penonaktifan pengguna pengguna aplikasi penting yang IDs sedang cuti berkepanjangan		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (d)	d) Di antara kontrol penting yang perlu dipertimbangkan adalah: - Proses sistematis penerapan dan otorisasi pembuatan pengguna IDs dan matriks kontrol akses - Melakukan penilaian risiko dan pemberian hak akses berdasarkan hal yang sama. - Implementasi kontrol akses berbasis peran yang dirancang untuk memastikan pemisahan tugas yang efektif - Mengubah nama pengguna default and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract - Proses untuk	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memberi tahu secara tepat waktu fungsi keamanan informasi mengenai penambaha n, penghapusan, dan perubahan peran pengguna - Rekonsili asi berkala pengguna IDs dalam suatu sistem dan pengguna aktual diharuskan memiliki akses dan penghapusan yang tidak perlu IDs, jika ada - Audit, pencatata n, dan pemantaua n akses ke aset TI oleh semua pengguna dan - Mempertim bangkan penonaktifan pengguna pengguna aplikasi penting yang IDs sedang cuti berkepanjangan		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (d)	d) Di antara kontrol penting yang perlu dipertimb angkan adalah: - Proses sistemati s penerapan dan otorisasi pembuatan pengguna IDs dan matriks kontrol akses - Melakukan penilaian risiko dan pemberian hak akses berdasark an hal yang sama. - Implementasi kontrol akses berbasis peran yang dirancang untuk memastika n pemisahan tugas yang efektif - Mengubah nama pengguna default and/or passwords of systems and prohibiti ng sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contrac t - Proses untuk	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memberi tahu secara tepat waktu fungsi keamanan informasi mengenai penambaha n, penghapusan, dan perubahan peran pengguna - Rekonsili asi berkala pengguna IDs dalam suatu sistem dan pengguna aktual diharuskan memiliki akses dan penghapusan yang tidak perlu IDs, jika ada - Audit, pencatata n, dan pemantaua n akses ke aset TI oleh semua pengguna dan - Mempertim bangkan penonaktifan pengguna pengguna aplikasi penting yang IDs sedang cuti berkepanjangan		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (d)	d) Di antara kontrol penting yang perlu dipertimb angkan adalah: - Proses sistemati s penerapan dan otorisasi pembuatan pengguna IDs dan matriks kontrol akses - Melakukan penilaian risiko dan pemberian hak akses berdasark an hal yang sama. - Implementasi kontrol akses berbasis peran yang dirancang untuk memastika n pemisahan tugas yang efektif - Mengubah nama pengguna default and/or passwords of systems and prohibiti ng sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contrac t - Proses untuk	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memberi tahu secara tepat waktu fungsi keamanan informasi mengenai penambahan, penghapusan, dan perubahan peran pengguna - Rekonsiliasi berkala pengguna IDs dalam suatu sistem dan pengguna aktual diharuskan memiliki akses dan penghapusan yang tidak perlu IDs, jika ada - Audit, pencatatan, dan pemantauan akses ke aset TI oleh semua pengguna dan - Mempertimbangkan penonaktifan pengguna pengguna aplikasi penting yang IDs sedang cuti berkepanjangan		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (d)	d) Di antara kontrol penting yang perlu dipertimb angkan adalah: - Proses sistemati s penerapan dan otorisasi pembuatan pengguna IDs dan matriks kontrol akses - Melakukan penilaian risiko dan pemberian hak akses berdasark an hal yang sama. - Implementasi kontrol akses berbasis peran yang dirancang untuk memastika n pemisahan tugas yang efektif - Mengubah nama pengguna default and/or passwords of systems and prohibiti ng sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contrac t - Proses untuk	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteks i aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memberi tahu secara tepat waktu fungsi keamanan informasi mengenai penambahan, penghapusan, dan perubahan peran pengguna - Rekonsiliasi berkala pengguna IDs dalam suatu sistem dan pengguna aktual diharuskan memiliki akses dan penghapusan yang tidak perlu IDs, jika ada - Audit, pencatatan, dan pemantauan akses ke aset TI oleh semua pengguna dan - Mempertimbangkan penonaktifan pengguna pengguna aplikasi penting yang IDs sedang cuti berkepanjangan		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (d)	d) Di antara kontrol penting yang perlu dipertimbangkan adalah: - Proses sistematis penerapan dan otorisasi pembuatan pengguna IDs dan matriks kontrol akses - Melakukan penilaian risiko dan pemberian hak akses berdasarkan hal yang sama. - Implementasi kontrol akses berbasis peran yang dirancang untuk memastikan pemisahan tugas yang efektif - Mengubah nama pengguna default and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract - Proses untuk	cloudwatch-alarm-action-check	Amazon CloudWatch mempertimbangkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memberi tahu secara tepat waktu fungsi keamanan informasi mengenai penambahan, penghapusan, dan perubahan peran pengguna - Rekonsiliasi berkala pengguna IDs dalam suatu sistem dan pengguna aktual diharuskan memiliki akses dan penghapusan yang tidak perlu IDs, jika ada - Audit, pencatatan, dan pemantauan akses ke aset TI oleh semua pengguna dan - Mempertimbangkan penonaktifan pengguna pengguna aplikasi penting yang IDs sedang cuti berkepanjangan		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (d)	d) Di antara kontrol penting yang perlu dipertimb angkan adalah: - Proses sistemati s penerapan dan otorisasi pembuatan pengguna IDs dan matriks kontrol akses - Melakukan penilaian risiko dan pemberian hak akses berdasark an hal yang sama. - Implementasi kontrol akses berbasis peran yang dirancang untuk memastika n pemisahan tugas yang efektif - Mengubah nama pengguna default and/or passwords of systems and prohibiti ng sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contrac t - Proses untuk	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memberi tahu secara tepat waktu fungsi keamanan informasi mengenai penambahan, penghapusan, dan perubahan peran pengguna - Rekonsiliasi berkala pengguna IDs dalam suatu sistem dan pengguna aktual diharuskan memiliki akses dan penghapusan yang tidak perlu IDs, jika ada - Audit, pencatatan, dan pemantauan akses ke aset TI oleh semua pengguna dan - Mempertimbangkan penonaktifan pengguna pengguna aplikasi penting yang IDs sedang cuti berkepanjangan		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (d)	d) Di antara kontrol penting yang perlu dipertimb angkan adalah: - Proses sistemati s penerapan dan otorisasi pembuatan pengguna IDs dan matriks kontrol akses - Melakukan penilaian risiko dan pemberian hak akses berdasark an hal yang sama. - Implementasi kontrol akses berbasis peran yang dirancang untuk memastika n pemisahan tugas yang efektif - Mengubah nama pengguna default and/or passwords of systems and prohibiti ng sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contrac t - Proses untuk	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memberi tahu secara tepat waktu fungsi keamanan informasi mengenai penambaha n, penghapusan, dan perubahan peran pengguna - Rekonsili asi berkala pengguna IDs dalam suatu sistem dan pengguna aktual diharuskan memiliki akses dan penghapusan yang tidak perlu IDs, jika ada - Audit, pencatata n, dan pemantaua n akses ke aset TI oleh semua pengguna dan - Mempertim bangkan penonaktifan pengguna pengguna aplikasi penting yang IDs sedang cuti berkepanjangan		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (d)	d) Di antara kontrol penting yang perlu dipertimb angkan adalah: - Proses sistemati s penerapan dan otorisasi pembuatan pengguna IDs dan matriks kontrol akses - Melakukan penilaian risiko dan pemberian hak akses berdasark an hal yang sama. - Implementasi kontrol akses berbasis peran yang dirancang untuk memastika n pemisahan tugas yang efektif - Mengubah nama pengguna default and/or passwords of systems and prohibiti ng sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contrac t - Proses untuk	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memberi tahu secara tepat waktu fungsi keamanan informasi mengenai penambahan, penghapusan, dan perubahan peran pengguna - Rekonsiliasi berkala pengguna IDs dalam suatu sistem dan pengguna aktual diharuskan memiliki akses dan penghapusan yang tidak perlu IDs, jika ada - Audit, pencatatan, dan pemantauan akses ke aset TI oleh semua pengguna dan - Mempertimbangkan penonaktifan pengguna pengguna aplikasi penting yang IDs sedang cuti berkepanjangan		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (d)	d) Di antara kontrol penting yang perlu dipertimb angkan adalah: - Proses sistemati s penerapan dan otorisasi pembuatan pengguna IDs dan matriks kontrol akses - Melakukan penilaian risiko dan pemberian hak akses berdasark an hal yang sama. - Implementasi kontrol akses berbasis peran yang dirancang untuk memastika n pemisahan tugas yang efektif - Mengubah nama pengguna default and/or passwords of systems and prohibiti ng sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contrac t - Proses untuk	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memberi tahu secara tepat waktu fungsi keamanan informasi mengenai penambahan, penghapusan, dan perubahan peran pengguna - Rekonsiliasi berkala pengguna IDs dalam suatu sistem dan pengguna aktual diharuskan memiliki akses dan penghapusan yang tidak perlu IDs, jika ada - Audit, pencatatan, dan pemantauan akses ke aset TI oleh semua pengguna dan - Mempertimbangkan penonaktifan pengguna pengguna aplikasi penting yang IDs sedang cuti berkepanjangan		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (d)	d) Di antara kontrol penting yang perlu dipertimb angkan adalah: - Proses sistemati s penerapan dan otorisasi pembuatan pengguna IDs dan matriks kontrol akses - Melakukan penilaian risiko dan pemberian hak akses berdasark an hal yang sama. - Implementasi kontrol akses berbasis peran yang dirancang untuk memastika n pemisahan tugas yang efektif - Mengubah nama pengguna default and/or passwords of systems and prohibiti ng sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contrac t - Proses untuk	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediak an metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinc i untuk permintaa n yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memberi tahu secara tepat waktu fungsi keamanan informasi mengenai penambahan, penghapusan, dan perubahan peran pengguna - Rekonsiliasi berkala pengguna IDs dalam suatu sistem dan pengguna aktual diharuskan memiliki akses dan penghapusan yang tidak perlu IDs, jika ada - Audit, pencatatan, dan pemantauan akses ke aset TI oleh semua pengguna dan - Mempertimbangkan penonaktifan pengguna pengguna aplikasi penting yang IDs sedang cuti berkepanjangan		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (d)	d) Di antara kontrol penting yang perlu dipertimb angkan adalah: - Proses sistemati s penerapan dan otorisasi pembuatan pengguna IDs dan matriks kontrol akses - Melakukan penilaian risiko dan pemberian hak akses berdasark an hal yang sama. - Implementasi kontrol akses berbasis peran yang dirancang untuk memastika n pemisahan tugas yang efektif - Mengubah nama pengguna default and/or passwords of systems and prohibiti ng sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contrac t - Proses untuk	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memberi tahu secara tepat waktu fungsi keamanan informasi mengenai penambahan, penghapusan, dan perubahan peran pengguna - Rekonsiliasi berkala pengguna IDs dalam suatu sistem dan pengguna aktual diharuskan memiliki akses dan penghapusan yang tidak perlu IDs, jika ada - Audit, pencatatan, dan pemantauan akses ke aset TI oleh semua pengguna dan - Mempertimbangkan penonaktifan pengguna pengguna aplikasi penting yang IDs sedang cuti berkepanjangan		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (d)	d) Di antara kontrol penting yang perlu dipertimb angkan adalah: - Proses sistemati s penerapan dan otorisasi pembuatan pengguna IDs dan matriks kontrol akses - Melakukan penilaian risiko dan pemberian hak akses berdasark an hal yang sama. - Implementasi kontrol akses berbasis peran yang dirancang untuk memastika n pemisahan tugas yang efektif - Mengubah nama pengguna default and/or passwords of systems and prohibiti ng sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contrac t - Proses untuk	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang pergi ke dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memberi tahu secara tepat waktu fungsi keamanan informasi mengenai penambaha n, penghapusan, dan perubahan peran pengguna - Rekonsili asi berkala pengguna IDs dalam suatu sistem dan pengguna aktual diharuskan memiliki akses dan penghapusan yang tidak perlu IDs, jika ada - Audit, pencatata n, dan pemantaua n akses ke aset TI oleh semua pengguna dan - Mempertim bangkan penonaktifan pengguna pengguna aplikasi penting yang IDs sedang cuti berkepanjangan		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (d)	d) Di antara kontrol penting yang perlu dipertimbangkan adalah: - Proses sistematis penerapan dan otorisasi pembuatan pengguna IDs dan matriks kontrol akses - Melakukan penilaian risiko dan pemberian hak akses berdasarkan hal yang sama. - Implementasi kontrol akses berbasis peran yang dirancang untuk memastikan pemisahan tugas yang efektif - Mengubah nama pengguna default and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract - Proses untuk	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memberi tahu secara tepat waktu fungsi keamanan informasi mengenai penambahan, penghapusan, dan perubahan peran pengguna - Rekonsiliasi berkala pengguna IDs dalam suatu sistem dan pengguna aktual diharuskan memiliki akses dan penghapusan yang tidak perlu IDs, jika ada - Audit, pencatatan, dan pemantauan akses ke aset TI oleh semua pengguna dan - Mempertimbangkan penonaktifan pengguna pengguna aplikasi penting yang IDs sedang cuti berkepanjangan		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (d)	d) Di antara kontrol penting yang perlu dipertimb angkan adalah: - Proses sistemati s penerapan dan otorisasi pembuatan pengguna IDs dan matriks kontrol akses - Melakukan penilaian risiko dan pemberian hak akses berdasark an hal yang sama. - Implementasi kontrol akses berbasis peran yang dirancang untuk memastika n pemisahan tugas yang efektif - Mengubah nama pengguna default and/or passwords of systems and prohibiti ng sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contrac t - Proses untuk	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memberi tahu secara tepat waktu fungsi keamanan informasi mengenai penambahan, penghapusan, dan perubahan peran pengguna - Rekonsiliasi berkala pengguna IDs dalam suatu sistem dan pengguna aktual diharuskan memiliki akses dan penghapusan yang tidak perlu IDs, jika ada - Audit, pencatatan, dan pemantauan akses ke aset TI oleh semua pengguna dan - Mempertimbangkan penonaktifan pengguna pengguna aplikasi penting yang IDs sedang cuti berkepanjangan		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (d)	d) Di antara kontrol penting yang perlu dipertimbangkan adalah: - Proses sistematis penerapan dan otorisasi pembuatan pengguna IDs dan matriks kontrol akses - Melakukan penilaian risiko dan pemberian hak akses berdasarkan hal yang sama. - Implementasi kontrol akses berbasis peran yang dirancang untuk memastikan pemisahan tugas yang efektif - Mengubah nama pengguna default and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract - Proses untuk	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memberi tahu secara tepat waktu fungsi keamanan informasi mengenai penambahan, penghapusan, dan perubahan peran pengguna - Rekonsiliasi berkala pengguna IDs dalam suatu sistem dan pengguna aktual diharuskan memiliki akses dan penghapusan yang tidak perlu IDs, jika ada - Audit, pencatatan, dan pemantauan akses ke aset TI oleh semua pengguna dan - Mempertimbangkan penonaktifan pengguna pengguna aplikasi penting yang IDs sedang cuti berkepanjangan		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (d)	d) Di antara kontrol penting yang perlu dipertimbangkan adalah: - Proses sistematis penerapan dan otorisasi pembuatan pengguna IDs dan matriks kontrol akses - Melakukan penilaian risiko dan pemberian hak akses berdasarkan hal yang sama. - Implementasi kontrol akses berbasis peran yang dirancang untuk memastikan pemisahan tugas yang efektif - Mengubah nama pengguna default and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract - Proses untuk	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memberi tahu secara tepat waktu fungsi keamanan informasi mengenai penambahan, penghapusan, dan perubahan peran pengguna - Rekonsiliasi berkala pengguna IDs dalam suatu sistem dan pengguna aktual diharuskan memiliki akses dan penghapusan yang tidak perlu IDs, jika ada - Audit, pencatatan, dan pemantauan akses ke aset TI oleh semua pengguna dan - Mempertimbangkan penonaktifan pengguna pengguna aplikasi penting yang IDs sedang cuti berkepanjangan		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (d)	d) Di antara kontrol penting yang perlu dipertimbangkan adalah: - Proses sistematis penerapan dan otorisasi pembuatan pengguna IDs dan matriks kontrol akses - Melakukan penilaian risiko dan pemberian hak akses berdasarkan hal yang sama. - Implementasi kontrol akses berbasis peran yang dirancang untuk memastikan pemisahan tugas yang efektif - Mengubah nama pengguna default and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract - Proses untuk	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memberi tahu secara tepat waktu fungsi keamanan informasi mengenai penambahan, penghapusan, dan perubahan peran pengguna - Rekonsiliasi berkala pengguna IDs dalam suatu sistem dan pengguna aktual diharuskan memiliki akses dan penghapusan yang tidak perlu IDs, jika ada - Audit, pencatatan, dan pemantauan akses ke aset TI oleh semua pengguna dan - Mempertimbangkan penonaktifan pengguna pengguna aplikasi penting yang IDs sedang cuti berkepanjangan		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (d)	d) Di antara kontrol penting yang perlu dipertimbangkan adalah: - Proses sistematis penerapan dan otorisasi pembuatan pengguna IDs dan matriks kontrol akses - Melakukan penilaian risiko dan pemberian hak akses berdasarkan hal yang sama. - Implementasi kontrol akses berbasis peran yang dirancang untuk memastikan pemisahan tugas yang efektif - Mengubah nama pengguna default and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract - Proses untuk	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memberi tahu secara tepat waktu fungsi keamanan informasi mengenai penambahan, penghapusan, dan perubahan peran pengguna - Rekonsiliasi berkala pengguna IDs dalam suatu sistem dan pengguna aktual diharuskan memiliki akses dan penghapusan yang tidak perlu IDs, jika ada - Audit, pencatatan, dan pemantauan akses ke aset TI oleh semua pengguna dan - Mempertimbangkan penonaktifan pengguna pengguna aplikasi penting yang IDs sedang cuti berkepanjangan		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (d)	d) Di antara kontrol penting yang perlu dipertimbangkan adalah: - Proses sistematis penerapan dan otorisasi pembuatan pengguna IDs dan matriks kontrol akses - Melakukan penilaian risiko dan pemberian hak akses berdasarkan hal yang sama. - Implementasi kontrol akses berbasis peran yang dirancang untuk memastikan pemisahan tugas yang efektif - Mengubah nama pengguna default and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract - Proses untuk	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memberi tahu secara tepat waktu fungsi keamanan informasi mengenai penambahan, penghapusan, dan perubahan peran pengguna - Rekonsiliasi berkala pengguna IDs dalam suatu sistem dan pengguna aktual diharuskan memiliki akses dan penghapusan yang tidak perlu IDs, jika ada - Audit, pencatatan, dan pemantauan akses ke aset TI oleh semua pengguna dan - Mempertimbangkan penonaktifan pengguna pengguna aplikasi penting yang IDs sedang cuti berkepanjangan		harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (d)	d) Di antara kontrol penting yang perlu dipertimbangkan adalah: - Proses sistematis penerapan dan otorisasi pembuatan pengguna IDs dan matriks kontrol akses - Melakukan penilaian risiko dan pemberian hak akses berdasarkan hal yang sama. - Implementasi kontrol akses berbasis peran yang dirancang untuk memastikan pemisahan tugas yang efektif - Mengubah nama pengguna default and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract - Proses untuk	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memberi tahu secara tepat waktu fungsi keamanan informasi mengenai penambaha n, penghapusan, dan perubahan peran pengguna - Rekonsili asi berkala pengguna IDs dalam suatu sistem dan pengguna aktual diharuskan memiliki akses dan penghapusan yang tidak perlu IDs, jika ada - Audit, pencatata n, dan pemantaua n akses ke aset TI oleh semua pengguna dan - Mempertim bangkan penonaktifan pengguna pengguna aplikasi penting yang IDs sedang cuti berkepanjangan		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (d)	d) Di antara kontrol penting yang perlu dipertimb angkan adalah: - Proses sistemati s penerapan dan otorisasi pembuatan pengguna IDs dan matriks kontrol akses - Melakukan penilaian risiko dan pemberian hak akses berdasark an hal yang sama. - Implementasi kontrol akses berbasis peran yang dirancang untuk memastika n pemisahan tugas yang efektif - Mengubah nama pengguna default and/or passwords of systems and prohibiti ng sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contrac t - Proses untuk	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memberi tahu secara tepat waktu fungsi keamanan informasi mengenai penambahan, penghapusan, dan perubahan peran pengguna - Rekonsiliasi berkala pengguna IDs dalam suatu sistem dan pengguna aktual diharuskan memiliki akses dan penghapusan yang tidak perlu IDs, jika ada - Audit, pencatatan, dan pemantauan akses ke aset TI oleh semua pengguna dan - Mempertimbangkan penonaktifan pengguna pengguna aplikasi penting yang IDs sedang cuti berkepanjangan		harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (d)	d) Di antara kontrol penting yang perlu dipertimbangkan adalah: - Proses sistematis penerapan dan otorisasi pembuatan pengguna IDs dan matriks kontrol akses - Melakukan penilaian risiko dan pemberian hak akses berdasarkan hal yang sama. - Implementasi kontrol akses berbasis peran yang dirancang untuk memastikan pemisahan tugas yang efektif - Mengubah nama pengguna default and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract - Proses untuk	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memberi tahu secara tepat waktu fungsi keamanan informasi mengenai penambahan, penghapusan, dan perubahan peran pengguna - Rekonsiliasi berkala pengguna IDs dalam suatu sistem dan pengguna aktual diharuskan memiliki akses dan penghapusan yang tidak perlu IDs, jika ada - Audit, pencatatan, dan pemantauan akses ke aset TI oleh semua pengguna dan - Mempertimbangkan penonaktifan pengguna pengguna aplikasi penting yang IDs sedang cuti berkepanjangan		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (d)	d) Di antara kontrol penting yang perlu dipertimb angkan adalah: - Proses sistemati s penerapan dan otorisasi pembuatan pengguna IDs dan matriks kontrol akses - Melakukan penilaian risiko dan pemberian hak akses berdasark an hal yang sama. - Implementasi kontrol akses berbasis peran yang dirancang untuk memastika n pemisahan tugas yang efektif - Mengubah nama pengguna default and/or passwords of systems and prohibiti ng sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contrac t - Proses untuk	ec2- instance-profile-a ttached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirk an profil instans ke instans Anda dapat membantu pengelola an hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memberi tahu secara tepat waktu fungsi keamanan informasi mengenai penambahan, penghapusan, dan perubahan peran pengguna - Rekonsiliasi berkala pengguna IDs dalam suatu sistem dan pengguna aktual diharuskan memiliki akses dan penghapusan yang tidak perlu IDs, jika ada - Audit, pencatatan, dan pemantauan akses ke aset TI oleh semua pengguna dan - Mempertimbangkan penonaktifan pengguna pengguna aplikasi penting yang IDs sedang cuti berkepanjangan		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (d)	d) Di antara kontrol penting yang perlu dipertimbangkan adalah: - Proses sistematis penerapan dan otorisasi pembuatan pengguna IDs dan matriks kontrol akses - Melakukan penilaian risiko dan pemberian hak akses berdasarkan hal yang sama. - Implementasi kontrol akses berbasis peran yang dirancang untuk memastikan pemisahan tugas yang efektif - Mengubah nama pengguna default and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract - Proses untuk	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memberi tahu secara tepat waktu fungsi keamanan informasi mengenai penambahan, penghapusan, dan perubahan peran pengguna - Rekonsiliasi berkala pengguna IDs dalam suatu sistem dan pengguna aktual diharuskan memiliki akses dan penghapusan yang tidak perlu IDs, jika ada - Audit, pencatatan, dan pemantauan akses ke aset TI oleh semua pengguna dan - Mempertimbangkan penonaktifan pengguna pengguna aplikasi penting yang IDs sedang cuti berkepanjangan		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (d)	d) Di antara kontrol penting yang perlu dipertimb angkan adalah: - Proses sistemati s penerapan dan otorisasi pembuatan pengguna IDs dan matriks kontrol akses - Melakukan penilaian risiko dan pemberian hak akses berdasark an hal yang sama. - Implementasi kontrol akses berbasis peran yang dirancang untuk memastika n pemisahan tugas yang efektif - Mengubah nama pengguna default and/or passwords of systems and prohibiti ng sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contrac t - Proses untuk	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memberi tahu secara tepat waktu fungsi keamanan informasi mengenai penambahan, penghapusan, dan perubahan peran pengguna - Rekonsiliasi berkala pengguna IDs dalam suatu sistem dan pengguna aktual diharuskan memiliki akses dan penghapusan yang tidak perlu IDs, jika ada - Audit, pencatatan, dan pemantauan akses ke aset TI oleh semua pengguna dan - Mempertimbangkan penonaktifan pengguna pengguna aplikasi penting yang IDs sedang cuti berkepanjangan		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (d)	d) Di antara kontrol penting yang perlu dipertimb angkan adalah: - Proses sistemati s penerapan dan otorisasi pembuatan pengguna IDs dan matriks kontrol akses - Melakukan penilaian risiko dan pemberian hak akses berdasark an hal yang sama. - Implementasi kontrol akses berbasis peran yang dirancang untuk memastika n pemisahan tugas yang efektif - Mengubah nama pengguna default and/or passwords of systems and prohibiti ng sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contrac t - Proses untuk	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memberi tahu secara tepat waktu fungsi keamanan informasi mengenai penambahan, penghapusan, dan perubahan peran pengguna - Rekonsiliasi berkala pengguna IDs dalam suatu sistem dan pengguna aktual diharuskan memiliki akses dan penghapusan yang tidak perlu IDs, jika ada - Audit, pencatatan, dan pemantauan akses ke aset TI oleh semua pengguna dan - Mempertimbangkan penonaktifan pengguna pengguna aplikasi penting yang IDs sedang cuti berkepanjangan		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (d)	d) Di antara kontrol penting yang perlu dipertimb angkan adalah: - Proses sistemati s penerapan dan otorisasi pembuatan pengguna IDs dan matriks kontrol akses - Melakukan penilaian risiko dan pemberian hak akses berdasark an hal yang sama. - Implementasi kontrol akses berbasis peran yang dirancang untuk memastika n pemisahan tugas yang efektif - Mengubah nama pengguna default and/or passwords of systems and prohibiti ng sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contrac t - Proses untuk	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	memberi tahu secara tepat waktu fungsi keamanan informasi mengenai penambahan, penghapusan, dan perubahan peran pengguna - Rekonsiliasi berkala pengguna IDs dalam suatu sistem dan pengguna aktual diharuskan memiliki akses dan penghapusan yang tidak perlu IDs, jika ada - Audit, pencatatan, dan pemantauan akses ke aset TI oleh semua pengguna dan - Mempertimbangkan penonaktifan pengguna pengguna aplikasi penting yang IDs sedang cuti berkepanjangan		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (f)	f) Untuk tujuan akuntabilitas, pastikan bahwa pengguna dan aset TI diidentif ikasi secara unik dan tindakan mereka dapat diaudit.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (f)	f) Untuk tujuan akuntabilitas, pastikan bahwa pengguna dan aset TI diidentif ikasi secara unik dan tindakan mereka dapat diaudit.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (f)	f) Untuk tujuan akuntabilitas, pastikan bahwa pengguna dan aset TI diidentif ikasi secara unik dan tindakan mereka dapat diaudit.	opensearch-audit-l ogging-enabled	Pastikan pencatata n audit diaktifkan di domain OpenSearc h Layanan Amazon Anda. Pencatatan audit memungkin kan Anda melacak aktivitas pengguna di OpenSearc h domain Anda, termasuk keberhasi lan dan kegagalan otentikasi, permintaa n, perubahan indeks OpenSearch, dan kueri penelusuran yang masuk.
3.1.1 (f)	f) Untuk tujuan akuntabilitas, pastikan bahwa pengguna dan aset TI diidentif ikasi secara unik dan tindakan mereka dapat diaudit.	redshift-audit-logging-enabled	Untuk menangkap informasi tentang koneksi dan aktivitas pengguna di klaster Amazon Redshift, pastikan pencatatan audit diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (f)	f) Untuk tujuan akuntabilitas, pastikan bahwa pengguna dan aset TI diidentif ikasi secara unik dan tindakan mereka dapat diaudit.	redshift-cluster-c onfiguration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastika n bahwa konfigura si yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberika n informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapka n untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (f)	f) Untuk tujuan akuntabilitas, pastikan bahwa pengguna dan aset TI diidentif ikasi secara unik dan tindakan mereka dapat diaudit.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.
3.1.1 (f)	f) Untuk tujuan akuntabilitas, pastikan bahwa pengguna dan aset TI diidentif ikasi secara unik dan tindakan mereka dapat diaudit.	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasark an fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahu an orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengotent ikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasark an fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahu an orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang pergi ke dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi, pengembalian, dan pendelegasian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasark an fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahu an orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1 (h)	h) Administrator sistem, petugas keamanan, programmer dan staf yang melakukan operasi kritis selalu memiliki kemampuan untuk menimbulkan kerusakan parah pada sistem keuangan yang mereka pertahankan atau operasikan berdasarkan fungsi pekerjaan mereka dan akses istimewa. Personil dengan hak akses sistem yang tinggi harus diawasi secara ketat dengan semua aktivitas sistem mereka dicatat, karena mereka memiliki pengetahuan orang dalam dan sumber daya untuk menghindari kontrol sistem dan prosedur keamanan. Beberapa praktik kontrol dan keamanan yang disebutkan di bawah ini perlu dipertimbangkan: -	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Menerapkan otentikasi dua faktor untuk pengguna istimewa - Melembagakan kontrol yang kuat atas akses jarak jauh oleh pengguna istimewa - Membatasi jumlah pengguna istimewa - Memberikan akses istimewa berdasarkan '' atau 'need-to-have' - Mempertahankan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna istimewa - Memastikan bahwa pengguna istimewa tidak memiliki akses ke log sistem di mana aktivitas mereka ditangkap - Melakukan audit rutin atau tinjauan manajemen need-to-do log - Melarang berbagi hak istimewa IDs dan kode aksesnya - Melarang vendor dan kontraktor mendapatkan akses istimewa ke sistem tanpa pengawasan dan pemantauan ketat		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	dan _ Melindungi data cadangan dari akses yang tidak sah		
3.1.2 (a)	a) BFI harus menginstal perangkat keamanan jaringan, seperti firewall, perangkat lunak anti-virus/anti-malware serta sistem deteksi dan pencegahan intrusi, pada titik kritis infrastruktur TI, untuk melindungi perimeter jaringan.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (a)	a) BFI harus menginstal perangkat keamanan jaringan, seperti firewall, perangkat lunak anti-virus/anti-malware serta sistem deteksi dan pencegahan intrusi, pada titik kritis infrastruktur TI, untuk melindungi perimeter jaringan.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (a)	a) BFI harus menginstal perangkat keamanan jaringan, seperti firewall, perangkat lunak anti-virus/anti-malware serta sistem deteksi dan pencegahan intrusi, pada titik kritis infrastruktur TI, untuk melindungi perimeter jaringan.	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindunginya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimbangkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapkan - Tanggung jawab operasional untuk jaringan harus dipisahkan dari operasi komputer jika sesuai - Kontrol khusus harus ditetapkan untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimbangkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapkan - Tanggung jawab operasional untuk jaringan harus dipisahkan dari operasi komputer jika sesuai - Kontrol khusus harus ditetapkan untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimbangkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapkan - Tanggung jawab operasional untuk jaringan harus dipisahkan dari operasi komputer jika sesuai - Kontrol khusus harus ditetapkan untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	alb-http-drop-invalid-header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimbangkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapkan - Tanggung jawab operasional untuk jaringan harus dipisahkan dari operasi komputer jika sesuai - Kontrol khusus harus ditetapkan untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimbangkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapkan - Tanggung jawab operasional untuk jaringan harus dipisahkan dari operasi komputer jika sesuai - Kontrol khusus harus ditetapkan untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimbangkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapkan - Tanggung jawab operasional untuk jaringan harus dipisahkan dari operasi komputer jika sesuai - Kontrol khusus harus ditetapkan untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimbangkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapkan - Tanggung jawab operasional untuk jaringan harus dipisahkan dari operasi komputer jika sesuai - Kontrol khusus harus ditetapkan untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimbangkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapkan - Tanggung jawab operasional untuk jaringan harus dipisahkan dari operasi komputer jika sesuai - Kontrol khusus harus ditetapkan untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	cloudwatch-alarm-action-check	Amazon CloudWatch memperingatkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimbangkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapkan - Tanggung jawab operasional untuk jaringan harus dipisahkan dari operasi komputer jika sesuai - Kontrol khusus harus ditetapkan untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimbangkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapkan - Tanggung jawab operasional untuk jaringan harus dipisahkan dari operasi komputer jika sesuai - Kontrol khusus harus ditetapkan untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimbangkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapkan - Tanggung jawab operasional untuk jaringan harus dipisahkan dari operasi komputer jika sesuai - Kontrol khusus harus ditetapkan untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimbangkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapkan - Tanggung jawab operasional untuk jaringan harus dipisahkan dari operasi komputer jika sesuai - Kontrol khusus harus ditetapkan untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimbangkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapkan - Tanggung jawab operasional untuk jaringan harus dipisahkan dari operasi komputer jika sesuai - Kontrol khusus harus ditetapkan untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimbangkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapkan - Tanggung jawab operasional untuk jaringan harus dipisahkan dari operasi komputer jika sesuai - Kontrol khusus harus ditetapkan untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimbangkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapkan - Tanggung jawab operasional untuk jaringan harus dipisahkan dari operasi komputer jika sesuai - Kontrol khusus harus ditetapkan untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimbangkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapkan - Tanggung jawab operasional untuk jaringan harus dipisahkan dari operasi komputer jika sesuai - Kontrol khusus harus ditetapkan untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	sagemaker-notebook -no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/ 0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurk an ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimbangkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapkan - Tanggung jawab operasional untuk jaringan harus dipisahkan dari operasi komputer jika sesuai - Kontrol khusus harus ditetapkan untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimbangkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapkan - Tanggung jawab operasional untuk jaringan harus dipisahkan dari operasi komputer jika sesuai - Kontrol khusus harus ditetapkan untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositori data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimb angkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapka n - Tanggung jawab operasion al untuk jaringan harus dipisahka n dari operasi komputer jika sesuai - Kontrol khusus harus ditetapka n untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimbangkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapkan - Tanggung jawab operasional untuk jaringan harus dipisahkan dari operasi komputer jika sesuai - Kontrol khusus harus ditetapkan untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimbangkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapkan - Tanggung jawab operasional untuk jaringan harus dipisahkan dari operasi komputer jika sesuai - Kontrol khusus harus ditetapkan untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimbangkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapkan - Tanggung jawab operasional untuk jaringan harus dipisahkan dari operasi komputer jika sesuai - Kontrol khusus harus ditetapkan untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (c)	c) Kontrol harus diterapkan untuk memastikan keamanan informasi dalam jaringan dan perlindungan layanan yang terhubung dari akses yang tidak sah. Secara khusus, hal-hal berikut harus dipertimbangkan: - Tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan harus ditetapkan - Tanggung jawab operasional untuk jaringan harus dipisahkan dari operasi komputer jika sesuai - Kontrol khusus harus ditetapkan untuk menjaga kerahasiaan dan integritas data yang melewati jaringan publik atau melalui jaringan nirkabel dan untuk melindungi sistem dan aplikasi yang terhubung (termasuk protokol	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	enkripsi jaringan saat menghubungkan ke sistem/jaringan yang tidak dipercaya . - Pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi - Kegiatan manajemen harus dikoordinasikan secara erat baik untuk mengoptim alkan layanan kepada organisasi dan untuk memastikan bahwa kontrol diterapkan secara konsisten di seluruh infrastru ktur pemrosesan informasi - Sistem pada jaringan harus diautentikasi dan - Koneksi sistem yang tidak tepercaya ke jaringan harus dibatasi		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (e)	e) Layanan jaringan dapat berkisar dari bandwidth sederhana yang tidak dikelola hingga layanan canggih seperti VPN, Voice over IP, VSAT, dll. Fitur keamanan layanan jaringan harus: - Teknologi diterapkan untuk keamanan layanan jaringan, seperti otentikasi, enkripsi dan kontrol koneksi jaringan - Parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan sesuai dengan aturan keamanan dan koneksi jaringan dan - Prosedur untuk penggunaan layanan jaringan untuk membatasi akses ke layanan jaringan atau aplikasi, jika diperlukan	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (e)	e) Layanan jaringan dapat berkisar dari bandwidth sederhana yang tidak dikelola hingga layanan canggih seperti VPN, Voice over IP, VSAT, dll. Fitur keamanan layanan jaringan harus: - Teknologi diterapkan untuk keamanan layanan jaringan, seperti otentikasi, enkripsi dan kontrol koneksi jaringan - Parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan sesuai dengan aturan keamanan dan koneksi jaringan dan - Prosedur untuk penggunaan layanan jaringan untuk membatasi akses ke layanan jaringan atau aplikasi, jika diperlukan	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (e)	e) Layanan jaringan dapat berkisar dari bandwidth sederhana yang tidak dikelola hingga layanan canggih seperti VPN, Voice over IP, VSAT, dll. Fitur keamanan layanan jaringan harus: - Teknologi diterapkan untuk keamanan layanan jaringan, seperti otentikasi, enkripsi dan kontrol koneksi jaringan - Parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan sesuai dengan aturan keamanan dan koneksi jaringan dan - Prosedur untuk penggunaan layanan jaringan untuk membatasi akses ke layanan jaringan atau aplikasi, jika diperlukan	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (e)	e) Layanan jaringan dapat berkisar dari bandwidth sederhana yang tidak dikelola hingga layanan canggih seperti VPN, Voice over IP, VSAT, dll. Fitur keamanan layanan jaringan harus: - Teknologi diterapkan untuk keamanan layanan jaringan, seperti otentikasi, enkripsi dan kontrol koneksi jaringan - Parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan sesuai dengan aturan keamanan dan koneksi jaringan dan - Prosedur untuk penggunaan layanan jaringan untuk membatasi akses ke layanan jaringan atau aplikasi, jika diperlukan	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (e)	e) Layanan jaringan dapat berkisar dari bandwidth sederhana yang tidak dikelola hingga layanan canggih seperti VPN, Voice over IP, VSAT, dll. Fitur keamanan layanan jaringan harus: - Teknologi diterapkan untuk keamanan layanan jaringan, seperti otentikasi, enkripsi dan kontrol koneksi jaringan - Parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan sesuai dengan aturan keamanan dan koneksi jaringan dan - Prosedur untuk penggunaan layanan jaringan untuk membatasi akses ke layanan jaringan atau aplikasi, jika diperlukan	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (e)	e) Layanan jaringan dapat berkisar dari bandwidth sederhana yang tidak dikelola hingga layanan canggih seperti VPN, Voice over IP, VSAT, dll. Fitur keamanan layanan jaringan harus: - Teknologi diterapkan untuk keamanan layanan jaringan, seperti otentikasi, enkripsi dan kontrol koneksi jaringan - Parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan sesuai dengan aturan keamanan dan koneksi jaringan dan - Prosedur untuk penggunaan layanan jaringan untuk membatasi akses ke layanan jaringan atau aplikasi, jika diperlukan	alb-http-drop-invalid-header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (e)	e) Layanan jaringan dapat berkisar dari bandwidth sederhana yang tidak dikelola hingga layanan canggih seperti VPN, Voice over IP, VSAT, dll. Fitur keamanan layanan jaringan harus: - Teknologi diterapkan untuk keamanan layanan jaringan, seperti otentikasi, enkripsi dan kontrol koneksi jaringan - Parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan sesuai dengan aturan keamanan dan koneksi jaringan dan - Prosedur untuk penggunaan layanan jaringan untuk membatasi akses ke layanan jaringan atau aplikasi, jika diperlukan	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (e)	e) Layanan jaringan dapat berkisar dari bandwidth sederhana yang tidak dikelola hingga layanan canggih seperti VPN, Voice over IP, VSAT, dll. Fitur keamanan layanan jaringan harus: - Teknologi diterapkan untuk keamanan layanan jaringan, seperti otentikasi, enkripsi dan kontrol koneksi jaringan - Parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan sesuai dengan aturan keamanan dan koneksi jaringan dan - Prosedur untuk penggunaan layanan jaringan untuk membatasi akses ke layanan jaringan atau aplikasi, jika diperlukan	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (e)	e) Layanan jaringan dapat berkisar dari bandwidth sederhana yang tidak dikelola hingga layanan canggih seperti VPN, Voice over IP, VSAT, dll. Fitur keamanan layanan jaringan harus: - Teknologi diterapkan untuk keamanan layanan jaringan, seperti otentikasi, enkripsi dan kontrol koneksi jaringan - Parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan sesuai dengan aturan keamanan dan koneksi jaringan dan - Prosedur untuk penggunaan layanan jaringan untuk membatasi akses ke layanan jaringan atau aplikasi, jika diperlukan	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (e)	e) Layanan jaringan dapat berkisar dari bandwidth sederhana yang tidak dikelola hingga layanan canggih seperti VPN, Voice over IP, VSAT, dll. Fitur keamanan layanan jaringan harus: - Teknologi diterapkan untuk keamanan layanan jaringan, seperti otentikasi, enkripsi dan kontrol koneksi jaringan - Parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan sesuai dengan aturan keamanan dan koneksi jaringan dan - Prosedur untuk penggunaan layanan jaringan untuk membatasi akses ke layanan jaringan atau aplikasi, jika diperlukan	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2 (e)	e) Layanan jaringan dapat berkisar dari bandwidth sederhana yang tidak dikelola hingga layanan canggih seperti VPN, Voice over IP, VSAT, dll. Fitur keamanan layanan jaringan harus: - Teknologi diterapkan untuk keamanan layanan jaringan, seperti otentikasi, enkripsi dan kontrol koneksi jaringan - Parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan sesuai dengan aturan keamanan dan koneksi jaringan dan - Prosedur untuk penggunaan layanan jaringan untuk membatasi akses ke layanan jaringan atau aplikasi, jika diperlukan	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3 (e)	e) Gunakan enkripsi untuk melindungi saluran komunikasi antara perangkat akses jarak jauh dan institusi untuk membatasi risiko yang terkait dengan spoofing jaringan.	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.
3.1.3 (e)	e) Gunakan enkripsi untuk melindungi saluran komunikasi antara perangkat akses jarak jauh dan institusi untuk membatasi risiko yang terkait dengan spoofing jaringan.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3 (e)	e) Gunakan enkripsi untuk melindungi saluran komunikasi antara perangkat akses jarak jauh dan institusi untuk membatasi risiko yang terkait dengan spoofing jaringan.	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
3.1.3 (e)	e) Gunakan enkripsi untuk melindungi saluran komunikasi antara perangkat akses jarak jauh dan institusi untuk membatasi risiko yang terkait dengan spoofing jaringan.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3 (e)	e) Gunakan enkripsi untuk melindungi saluran komunikasi antara perangkat akses jarak jauh dan institusi untuk membatasi risiko yang terkait dengan spoofing jaringan.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
3.1.3 (e)	e) Gunakan enkripsi untuk melindungi saluran komunikasi antara perangkat akses jarak jauh dan institusi untuk membatasi risiko yang terkait dengan spoofing jaringan.	alb-http-drop-invalid-header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3 (e)	e) Gunakan enkripsi untuk melindungi saluran komunikasi antara perangkat akses jarak jauh dan institusi untuk membatasi risiko yang terkait dengan spoofing jaringan.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3 (e)	e) Gunakan enkripsi untuk melindungi saluran komunikasi antara perangkat akses jarak jauh dan institusi untuk membatasi risiko yang terkait dengan spoofing jaringan.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
3.1.3 (e)	e) Gunakan enkripsi untuk melindungi saluran komunikasi antara perangkat akses jarak jauh dan institusi untuk membatasi risiko yang terkait dengan spoofing jaringan.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3 (e)	e) Gunakan enkripsi untuk melindungi saluran komunikasi antara perangkat akses jarak jauh dan institusi untuk membatasi risiko yang terkait dengan spoofing jaringan.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.
3.1.3 (e)	e) Gunakan enkripsi untuk melindungi saluran komunikasi antara perangkat akses jarak jauh dan institusi untuk membatasi risiko yang terkait dengan spoofing jaringan.	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3 (g)	g) Menjaga log untuk komunikasi akses jarak jauh. Log harus mencakup tanggal, waktu, pengguna, lokasi pengguna, durasi, dan tujuan untuk semua akses jarak jauh termasuk semua aktivitas yang dilakukan melalui akses jarak jauh	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
3.1.3 (g)	g) Menjaga log untuk komunikasi akses jarak jauh. Log harus mencakup tanggal, waktu, pengguna, lokasi pengguna, durasi, dan tujuan untuk semua akses jarak jauh termasuk semua aktivitas yang dilakukan melalui akses jarak jauh	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3 (g)	g) Menjaga log untuk komunikasi akses jarak jauh. Log harus mencakup tanggal, waktu, pengguna, lokasi pengguna, durasi, dan tujuan untuk semua akses jarak jauh termasuk semua aktivitas yang dilakukan melalui akses jarak jauh	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
3.1.3 (g)	g) Menjaga log untuk komunikasi akses jarak jauh. Log harus mencakup tanggal, waktu, pengguna, lokasi pengguna, durasi, dan tujuan untuk semua akses jarak jauh termasuk semua aktivitas yang dilakukan melalui akses jarak jauh	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3 (g)	g) Menjaga log untuk komunikasi akses jarak jauh. Log harus mencakup tanggal, waktu, pengguna, lokasi pengguna, durasi, dan tujuan untuk semua akses jarak jauh termasuk semua aktivitas yang dilakukan melalui akses jarak jauh	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3 (g)	g) Menjaga log untuk komunikasi akses jarak jauh. Log harus mencakup tanggal, waktu, pengguna, lokasi pengguna, durasi, dan tujuan untuk semua akses jarak jauh termasuk semua aktivitas yang dilakukan melalui akses jarak jauh	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3 (g)	g) Menjaga log untuk komunikasi akses jarak jauh. Log harus mencakup tanggal, waktu, pengguna, lokasi pengguna, durasi, dan tujuan untuk semua akses jarak jauh termasuk semua aktivitas yang dilakukan melalui akses jarak jauh	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3 (g)	g) Menjaga log untuk komunikasi akses jarak jauh. Log harus mencakup tanggal, waktu, pengguna, lokasi pengguna, durasi, dan tujuan untuk semua akses jarak jauh termasuk semua aktivitas yang dilakukan melalui akses jarak jauh	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang pergi ke dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
3.1.3 (g)	g) Menjaga log untuk komunikasi akses jarak jauh. Log harus mencakup tanggal, waktu, pengguna, lokasi pengguna, durasi, dan tujuan untuk semua akses jarak jauh termasuk semua aktivitas yang dilakukan melalui akses jarak jauh	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3 (g)	g) Menjaga log untuk komunikasi akses jarak jauh. Log harus mencakup tanggal, waktu, pengguna, lokasi pengguna, durasi, dan tujuan untuk semua akses jarak jauh termasuk semua aktivitas yang dilakukan melalui akses jarak jauh	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3 (g)	g) Menjaga log untuk komunikasi akses jarak jauh. Log harus mencakup tanggal, waktu, pengguna, lokasi pengguna, durasi, dan tujuan untuk semua akses jarak jauh termasuk semua aktivitas yang dilakukan melalui akses jarak jauh	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3 (g)	g) Menjaga log untuk komunikasi akses jarak jauh. Log harus mencakup tanggal, waktu, pengguna, lokasi pengguna, durasi, dan tujuan untuk semua akses jarak jauh termasuk semua aktivitas yang dilakukan melalui akses jarak jauh	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3 (g)	g) Menjaga log untuk komunikasi akses jarak jauh. Log harus mencakup tanggal, waktu, pengguna, lokasi pengguna, durasi, dan tujuan untuk semua akses jarak jauh termasuk semua aktivitas yang dilakukan melalui akses jarak jauh	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.
3.1.3 (g)	g) Menjaga log untuk komunikasi akses jarak jauh. Log harus mencakup tanggal, waktu, pengguna, lokasi pengguna, durasi, dan tujuan untuk semua akses jarak jauh termasuk semua aktivitas yang dilakukan melalui akses jarak jauh	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3 (i)	i) Menerapkan proses otentikasi dua faktor untuk akses jarak jauh (misalnya, kartu token berbasis PIN dengan generator kata sandi acak satu kali, atau PKI berbasis token)	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3 (i)	i) Menerapkan proses otentikasi dua faktor untuk akses jarak jauh (misalnya, kartu token berbasis PIN dengan generator kata sandi acak satu kali, atau PKI berbasis token)	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3 (i)	i) Menerapkan proses otentikasi dua faktor untuk akses jarak jauh (misalnya, kartu token berbasis PIN dengan generator kata sandi acak satu kali, atau PKI berbasis token)	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3 (i)	i) Menerapkan proses otentikasi dua faktor untuk akses jarak jauh (misalnya, kartu token berbasis PIN dengan generator kata sandi acak satu kali, atau PKI berbasis token)	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.4 (c) (e)	c) Proses manajemen tambalan harus mencakup aspek-aspek seperti: - Menentukan metode untuk memperoleh dan memvalidasi tambalan untuk memastikan bahwa tambalan berasal dari sumber resmi - Mengidentifikasi kerentanan yang berlaku untuk aplikasi dan sistem yang digunakan oleh organisasi - Menilai dampak bisnis dari penerapan tambalan (atau tidak menerapkan tambalan tertentu) - Memastikan tambalan diuji - Menjelaskan metode untuk menyebarkan tambalan, misalnya secara otomatis - Melaporkan status penyebaran tambalan di seluruh organisasi dan - Termasuk metode untuk menangani penerapan tambalan	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	yang gagal (misalnya , pemindahan tambalan). e) BFIs harus menggunak an alat manajemen tambalan otomatis dan alat pembaruan perangkat lunak untuk semua sistem yang alatnya tersedia dan aman		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.4 (c) (e)	c) Proses manajemen tambalan harus mencakup aspek-aspek seperti: - Menentukan metode untuk memperoleh dan memvalidasi tambalan untuk memastikan bahwa tambalan berasal dari sumber resmi - Mengidentifikasi kerentanan yang berlaku untuk aplikasi dan sistem yang digunakan oleh organisasi - Menilai dampak bisnis dari penerapan tambalan (atau tidak menerapkan tambalan tertentu) - Memastikan tambalan diuji - Menjelaskan metode untuk menyebarkan tambalan, misalnya secara otomatis - Melaporkan status penyebaran tambalan di seluruh organisasi dan - Termasuk metode untuk menangani penerapan tambalan	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	yang gagal (misalnya , pemindahan tambalan). e) BFIs harus menggunak an alat manajemen tambalan otomatis dan alat pembaruan perangkat lunak untuk semua sistem yang alatnya tersedia dan aman		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.4 (c) (e)	c) Proses manajemen tambalan harus mencakup aspek-aspek seperti: - Menentukan metode untuk memperoleh dan memvalidasi tambalan untuk memastikan bahwa tambalan berasal dari sumber resmi - Mengidentifikasi kerentanan yang berlaku untuk aplikasi dan sistem yang digunakan oleh organisasi - Menilai dampak bisnis dari penerapan tambalan (atau tidak menerapkan tambalan tertentu) - Memastikan tambalan diuji - Menjelaskan metode untuk menyebarkan tambalan, misalnya secara otomatis - Melaporkan status penyebaran tambalan di seluruh organisasi dan - Termasuk metode untuk menangani penerapan tambalan	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	yang gagal (misalnya , pemindahan tambalan). e) BFIs harus menggunak an alat manajemen tambalan otomatis dan alat pembaruan perangkat lunak untuk semua sistem yang alatnya tersedia dan aman		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.4 (c) (e)	c) Proses manajemen tambalan harus mencakup aspek-aspek seperti: - Menentukan metode untuk memperoleh dan memvalidasi tambalan untuk memastikan bahwa tambalan berasal dari sumber resmi - Mengidentifikasi kerentanan yang berlaku untuk aplikasi dan sistem yang digunakan oleh organisasi - Menilai dampak bisnis dari penerapan tambalan (atau tidak menerapkan tambalan tertentu) - Memastikan tambalan diuji - Menjelaskan metode untuk menyebarkan tambalan, misalnya secara otomatis - Melaporkan status penyebaran tambalan di seluruh organisasi dan - Termasuk metode untuk menangani penerapan tambalan	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	yang gagal (misalnya , pemindahan tambalan). e) BFIs harus menggunak an alat manajemen tambalan otomatis dan alat pembaruan perangkat lunak untuk semua sistem yang alatnya tersedia dan aman		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.4 (c) (e)	c) Proses manajemen tambalan harus mencakup aspek-aspek seperti: - Menentukan metode untuk memperoleh dan memvalidasi tambalan untuk memastikan bahwa tambalan berasal dari sumber resmi - Mengidentifikasi kerentanan yang berlaku untuk aplikasi dan sistem yang digunakan oleh organisasi - Menilai dampak bisnis dari penerapan tambalan (atau tidak menerapkan tambalan tertentu) - Memastikan tambalan diuji - Menjelaskan metode untuk menyebarkan tambalan, misalnya secara otomatis - Melaporkan status penyebaran tambalan di seluruh organisasi dan - Termasuk metode untuk menangani penerapan tambalan	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	yang gagal (misalnya , pemindahan tambalan). e) BFIs harus menggunak an alat manajemen tambalan otomatis dan alat pembaruan perangkat lunak untuk semua sistem yang alatnya tersedia dan aman		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.4 (c) (e)	c) Proses manajemen tambalan harus mencakup aspek-aspek seperti: - Menentukan metode untuk memperoleh dan memvalidasi tambalan untuk memastikan bahwa tambalan berasal dari sumber resmi - Mengidentifikasi kerentanan yang berlaku untuk aplikasi dan sistem yang digunakan oleh organisasi - Menilai dampak bisnis dari penerapan tambalan (atau tidak menerapkan tambalan tertentu) - Memastikan tambalan diuji - Menjelaskan metode untuk menyebarkan tambalan, misalnya secara otomatis - Melaporkan status penyebaran tambalan di seluruh organisasi dan - Termasuk metode untuk menangani penerapan tambalan	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relational Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	yang gagal (misalnya , pemindahan tambalan). e) BFIs harus menggunak an alat manajemen tambalan otomatis dan alat pembaruan perangkat lunak untuk semua sistem yang alatnya tersedia dan aman		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.5 (d) (e)	d) Manajemen kunci yang tepat memerlukan proses yang aman untuk menghasilkan, menyimpan, mengarsipkan, mengambil, mendistribusikan, menghentikan dan menghancurkan kunci kriptografi e) Semua kunci kriptografi harus dilindungi dari modifikasi dan kerugian. Selain itu, kunci rahasia dan pribadi membutuhkan perlindungan terhadap penggunaan yang tidak sah serta pengungkapan. Peralatan yang digunakan untuk menghasilkan, menyimpan, dan mengarsipkan kunci harus dilindungi secara fisik	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.5 (d) (e)	d) Manajemen kunci yang tepat memerlukan proses yang aman untuk menghasilkan, menyimpan, mengarsipkan, mengambil, mendistribusikan, menghentikan dan menghancurkan kunci kriptografi e) Semua kunci kriptografi harus dilindungi dari modifikasi dan kerugian. Selain itu, kunci rahasia dan pribadi membutuhkan perlindungan terhadap penggunaan yang tidak sah serta pengungkapan. Peralatan yang digunakan untuk menghasilkan, menyimpan, dan mengarsipkan kunci harus dilindungi secara fisik	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.5 (d) (e)	d) Manajemen kunci yang tepat memerlukan proses yang aman untuk menghasilkan, menyimpan, mengarsipkan, mengambil, mendistribusikan, menghentikan dan menghancurkan kunci kriptografi e) Semua kunci kriptografi harus dilindungi dari modifikasi dan kerugian. Selain itu, kunci rahasia dan pribadi membutuhkan perlindungan terhadap penggunaan yang tidak sah serta pengungkapan. Peralatan yang digunakan untuk menghasilkan, menyimpan, dan mengarsipkan kunci harus dilindungi secara fisik	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.5 (d) (e)	d) Manajemen kunci yang tepat memerlukan proses yang aman untuk menghasilkan, menyimpan, mengarsipkan, mengambil, mendistribusikan, menghentikan dan menghancurkan kunci kriptografi e) Semua kunci kriptografi harus dilindungi dari modifikasi dan kerugian. Selain itu, kunci rahasia dan pribadi membutuhkan perlindungan terhadap penggunaan yang tidak sah serta pengungkapan. Peralatan yang digunakan untuk menghasilkan, menyimpan, dan mengarsipkan kunci harus dilindungi secara fisik	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi, pengembalian, dan pendelegasian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.5 (f)	f) Sistem manajemen kunci harus didasarkan pada seperangkat standar, prosedur, dan metode aman yang disepakati untuk: - menghasilkan kunci untuk sistem kriptografi yang berbeda dan aplikasi yang berbeda - menerbitkan dan memperoleh sertifikat kunci publik - mendistribusikan kunci ke entitas yang dituju, termasuk bagaimana kunci harus diaktifkan saat diterima - menyimpan kunci, termasuk bagaimana pengguna yang berwenang memperoleh akses ke kunci - mengubah atau memperbarui kunci termasuk aturan kapan kunci harus diubah dan bagaimana ini akan dilakukan - berurusan dengan dikompromikan kunci - mencabut kunci termasuk kunci bagaimana harus	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	ditarik atau dinonaktifkan, misalnya ketika kunci telah disusupi atau ketika pengguna meninggalkan organisasi (dalam hal ini kunci juga harus diarsipkan) - memulihkan kunci yang hilang atau rusak - mencadangkan atau mengarsipkan kunci - menghancurkan kunci, dan - logging dan audit aktivitas terkait manajemen kunci.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.5 (f)	f) Sistem manajemen kunci harus didasarkan pada seperangkat standar, prosedur, dan metode aman yang disepakati untuk: - menghasilkan kunci untuk sistem kriptografi yang berbeda dan aplikasi yang berbeda - menerbitkan dan memperoleh sertifikat kunci publik - mendistribusikan kunci ke entitas yang dituju, termasuk bagaimana kunci harus diaktifkan saat diterima - menyimpan kunci, termasuk bagaimana pengguna yang berwenang memperoleh akses ke kunci - mengubah atau memperbarui kunci termasuk aturan kapan kunci harus diubah dan bagaimana ini akan dilakukan - berurusan dengan dikompromikan kunci - mencabut kunci termasuk kunci bagaimana harus	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	ditarik atau dinonaktifkan, misalnya ketika kunci telah disusupi atau ketika pengguna meninggalkan organisasi (dalam hal ini kunci juga harus diarsipkan) - memulihkan kunci yang hilang atau rusak - mencadangkan atau mengarsipkan kunci - menghancurkan kunci, dan - logging dan audit aktivitas terkait manajemen kunci.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.5 (f)	f) Sistem manajemen kunci harus didasarkan pada seperangkat standar, prosedur, dan metode aman yang disepakati untuk: - menghasilkan kunci untuk sistem kriptografi yang berbeda dan aplikasi yang berbeda - menerbitkan dan memperoleh sertifikat kunci publik - mendistribusikan kunci ke entitas yang dituju, termasuk bagaimana kunci harus diaktifkan saat diterima - menyimpan kunci, termasuk bagaimana pengguna yang berwenang memperoleh akses ke kunci - mengubah atau memperbarui kunci termasuk aturan kapan kunci harus diubah dan bagaimana ini akan dilakukan - berurusan dengan dikompromikan kunci - mencabut kunci termasuk kunci bagaimana harus	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	ditarik atau dinonaktifkan, misalnya ketika kunci telah disusupi atau ketika pengguna meninggalkan organisasi (dalam hal ini kunci juga harus diarsipkan) - memulihkan kunci yang hilang atau rusak - mencadangkan atau mengarsipkan kunci - menghancurkan kunci, dan - logging dan audit aktivitas terkait manajemen kunci.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.5 (f)	f) Sistem manajemen kunci harus didasarkan pada seperangkat standar, prosedur, dan metode aman yang disepakati untuk: - menghasilkan kunci untuk sistem kriptografi yang berbeda dan aplikasi yang berbeda - menerbitkan dan memperoleh sertifikat kunci publik - mendistribusikan kunci ke entitas yang dituju, termasuk bagaimana kunci harus diaktifkan saat diterima - menyimpan kunci, termasuk bagaimana pengguna yang berwenang memperoleh akses ke kunci - mengubah atau memperbarui kunci termasuk aturan kapan kunci harus diubah dan bagaimana ini akan dilakukan - berurusan dengan dikompromikan kunci - mencabut kunci termasuk kunci bagaimana harus	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	ditarik atau dinonaktifkan, misalnya ketika kunci telah disusupi atau ketika pengguna meninggalkan organisasi (dalam hal ini kunci juga harus diarsipkan) - memulihkan kunci yang hilang atau rusak - mencadangkan atau mengarsipkan kunci - menghancurkan kunci, dan - logging dan audit aktivitas terkait manajemen kunci.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.5 (f)	f) Sistem manajemen kunci harus didasarkan pada seperangkat standar, prosedur, dan metode aman yang disepakati untuk: - menghasilkan kunci untuk sistem kriptografi yang berbeda dan aplikasi yang berbeda - menerbitkan dan memperoleh sertifikat kunci publik - mendistribusikan kunci ke entitas yang dituju, termasuk bagaimana kunci harus diaktifkan saat diterima - menyimpan kunci, termasuk bagaimana pengguna yang berwenang memperoleh akses ke kunci - mengubah atau memperbarui kunci termasuk aturan kapan kunci harus diubah dan bagaimana ini akan dilakukan - berurusan dengan dikompromikan kunci - mencabut kunci termasuk kunci bagaimana harus	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	ditarik atau dinonaktifkan, misalnya ketika kunci telah disusupi atau ketika pengguna meninggalkan organisasi (dalam hal ini kunci juga harus diarsipkan) - memulihkan kunci yang hilang atau rusak - mencadangkan atau mengarsipkan kunci - menghancurkan kunci, dan - logging dan audit aktivitas terkait manajemen kunci.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.5 (f)	f) Sistem manajemen kunci harus didasarkan pada seperangkat standar, prosedur, dan metode aman yang disepakati untuk: - menghasilkan kunci untuk sistem kriptografi yang berbeda dan aplikasi yang berbeda - menerbitkan dan memperoleh sertifikat kunci publik - mendistribusikan kunci ke entitas yang dituju, termasuk bagaimana kunci harus diaktifkan saat diterima - menyimpan kunci, termasuk bagaimana pengguna yang berwenang memperoleh akses ke kunci - mengubah atau memperbarui kunci termasuk aturan kapan kunci harus diubah dan bagaimana ini akan dilakukan - berurusan dengan dikompromikan kunci - mencabut kunci termasuk kunci bagaimana harus	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	ditarik atau dinonaktifkan, misalnya ketika kunci telah disusupi atau ketika pengguna meninggalkan organisasi (dalam hal ini kunci juga harus diarsipkan) - memulihkan kunci yang hilang atau rusak - mencadangkan atau mengarsipkan kunci - menghancurkan kunci, dan - logging dan audit aktivitas terkait manajemen kunci.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.5 (f)	f) Sistem manajemen kunci harus didasarkan pada seperangkat standar, prosedur, dan metode aman yang disepakati untuk: - menghasilkan kunci untuk sistem kriptografi yang berbeda dan aplikasi yang berbeda - menerbitkan dan memperoleh sertifikat kunci publik - mendistribusikan kunci ke entitas yang dituju, termasuk bagaimana kunci harus diaktifkan saat diterima - menyimpan kunci, termasuk bagaimana pengguna yang berwenang memperoleh akses ke kunci - mengubah atau memperbarui kunci termasuk aturan kapan kunci harus diubah dan bagaimana ini akan dilakukan - berurusan dengan dikompromikan kunci - mencabut kunci termasuk kunci bagaimana harus	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	ditarik atau dinonaktifkan, misalnya ketika kunci telah disusupi atau ketika pengguna meninggalkan organisasi (dalam hal ini kunci juga harus diarsipkan) - memulihkan kunci yang hilang atau rusak - mencadangkan atau mengarsipkan kunci - menghancurkan kunci, dan - logging dan audit aktivitas terkait manajemen kunci.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.6 (a)	a) BFI harus menggunakan kombinasi alat otomatis dan teknik manual untuk melakukan VA komprehensif secara berkala. Untuk sistem menghadap eksternal berbasis web, ruang lingkup VA harus mencakup kerentana n web umum seperti injeksi SQL dan skrip lintas situs.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.6 (a)	a) BFI harus menggunakan kombinasi alat otomatis dan teknik manual untuk melakukan VA komprehensif secara berkala. Untuk sistem menghadap eksternal berbasis web, ruang lingkup VA harus mencakup kerentana n web umum seperti injeksi SQL dan skrip lintas situs.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.6 (a)	a) BFI harus menggunakan kombinasi alat otomatis dan teknik manual untuk melakukan VA komprehensif secara berkala. Untuk sistem menghadap eksternal berbasis web, ruang lingkup VA harus mencakup kerentana n web umum seperti injeksi SQL dan skrip lintas situs.	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizink an, memblokir, atau menghitung permintaa n web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindung inya dari serangan berbahaya
3.1.6 (c)	c) BFI harus menetapkan proses untuk memulihkan masalah yang diidentif ikasi dalam VA & PT dan melakukan validasi ulang remediasi berikutny a untuk memvalida si bahwa kesenjang an telah ditangani sepenuhnya.	vuln-mitigated-acc epted(Pemeriksaan Proses)	Pastikan kerentana n yang baru diidentif ikasi diperbaiki atau didokumentasikan sebagai risiko yang diterima. Kerentana n harus diperbaik i atau diterima sebagai risiko sesuai dengan persyaratan kepatuhan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.6 (f)	f) Fungsi keamanan harus memberikan pembaruan status mengenai jumlah kerentanan kritis yang tidak tanggung-tanggung, untuk setiap departemen/divisi, dan rencana untuk mitigasi manajemen senior secara berkala	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.8	Pelatihan dan kesadaran pengguna	security-awareness-program-exists(Pemeriksaan Proses)	Membangun dan memelihara program kesadaran keamanan untuk organisasi Anda. Program kesadaran keamanan mendidik karyawan tentang cara melindungi organisasi mereka dari berbagai pelanggaran atau insiden keamanan.
3.1.10 (b)	b) Informasi sensitif seperti dokumentasi sistem, kode sumber aplikasi, dan data transaksi produksi harus memiliki kontrol yang lebih luas untuk mencegah perubahan (misalnya, pemeriksa integritas, hash kriptografi). Selain itu, kebijakan harus meminimalkan distribusi informasi sensitif, termasuk cetakan yang berisi informasi.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.10 (b)	b) Informasi sensitif seperti dokumentasi sistem, kode sumber aplikasi, dan data transaksi produksi harus memiliki kontrol yang lebih luas untuk mencegah perubahan (misalnya , pemeriksa integrita s, hash kriptografi). Selain itu, kebijakan harus meminimalkan distribusi informasi sensitif, termasuk cetakan yang berisi informasi.	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.10 (b)	b) Informasi sensitif seperti dokumentasi sistem, kode sumber aplikasi, dan data transaksi produksi harus memiliki kontrol yang lebih luas untuk mencegah perubahan (misalnya , pemeriksa integrita s, hash kriptografi). Selain itu, kebijakan harus meminimalkan distribusi informasi sensitif, termasuk cetakan yang berisi informasi.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus, atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.10 (b)	b) Informasi sensitif seperti dokumentasi sistem, kode sumber aplikasi, dan data transaksi produksi harus memiliki kontrol yang lebih luas untuk mencegah perubahan (misalnya , pemeriksa integrita s, hash kriptografi). Selain itu, kebijakan harus meminimalkan distribusi informasi sensitif, termasuk cetakan yang berisi informasi.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.10 (b)	b) Informasi sensitif seperti dokumentasi sistem, kode sumber aplikasi, dan data transaksi produksi harus memiliki kontrol yang lebih luas untuk mencegah perubahan (misalnya, pemeriksa integritas, hash kriptografi). Selain itu, kebijakan harus meminimalkan distribusi informasi sensitif, termasuk cetakan yang berisi informasi.	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.10 (b)	b) Informasi sensitif seperti dokumentasi sistem, kode sumber aplikasi, dan data transaksi produksi harus memiliki kontrol yang lebih luas untuk mencegah perubahan (misalnya, pemeriksa integritas, hash kriptografi). Selain itu, kebijakan harus meminimalkan distribusi informasi sensitif, termasuk cetakan yang berisi informasi.	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.10 (b)	b) Informasi sensitif seperti dokumentasi sistem, kode sumber aplikasi, dan data transaksi produksi harus memiliki kontrol yang lebih luas untuk mencegah perubahan (misalnya, pemeriksa integritas, hash kriptografi). Selain itu, kebijakan harus meminimalkan distribusi informasi sensitif, termasuk cetakan yang berisi informasi.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.10 (b)	b) Informasi sensitif seperti dokumentasi sistem, kode sumber aplikasi, dan data transaksi produksi harus memiliki kontrol yang lebih luas untuk mencegah perubahan (misalnya , pemeriksa integrita s, hash kriptografi). Selain itu, kebijakan harus meminimalkan distribusi informasi sensitif, termasuk cetakan yang berisi informasi.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.10 (b)	b) Informasi sensitif seperti dokumentasi sistem, kode sumber aplikasi, dan data transaksi produksi harus memiliki kontrol yang lebih luas untuk mencegah perubahan (misalnya, pemeriksa integritas, hash kriptografi). Selain itu, kebijakan harus meminimalkan distribusi informasi sensitif, termasuk cetakan yang berisi informasi.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.10 (b)	b) Informasi sensitif seperti dokumentasi sistem, kode sumber aplikasi, dan data transaksi produksi harus memiliki kontrol yang lebih luas untuk mencegah perubahan (misalnya , pemeriksa integrita s, hash kriptografi). Selain itu, kebijakan harus meminimalkan distribusi informasi sensitif, termasuk cetakan yang berisi informasi.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.10 (b)	b) Informasi sensitif seperti dokumentasi sistem, kode sumber aplikasi, dan data transaksi produksi harus memiliki kontrol yang lebih luas untuk mencegah perubahan (misalnya , pemeriksa integrita s, hash kriptografi). Selain itu, kebijakan harus meminimalkan distribusi informasi sensitif, termasuk cetakan yang berisi informasi.	sagemaker-endpoint -configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.10 (b)	b) Informasi sensitif seperti dokumentasi sistem, kode sumber aplikasi, dan data transaksi produksi harus memiliki kontrol yang lebih luas untuk mencegah perubahan (misalnya , pemeriksa integrita s, hash kriptografi). Selain itu, kebijakan harus meminimalkan distribusi informasi sensitif, termasuk cetakan yang berisi informasi.	sagemaker-notebook -instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.10 (b)	b) Informasi sensitif seperti dokumentasi sistem, kode sumber aplikasi, dan data transaksi produksi harus memiliki kontrol yang lebih luas untuk mencegah perubahan (misalnya , pemeriksa integrita s, hash kriptografi). Selain itu, kebijakan harus meminimalkan distribusi informasi sensitif, termasuk cetakan yang berisi informasi.	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.10 (b)	b) Informasi sensitif seperti dokumentasi sistem, kode sumber aplikasi, dan data transaksi produksi harus memiliki kontrol yang lebih luas untuk mencegah perubahan (misalnya , pemeriksa integrita s, hash kriptografi). Selain itu, kebijakan harus meminimalkan distribusi informasi sensitif, termasuk cetakan yang berisi informasi.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.10 (b)	b) Informasi sensitif seperti dokumentasi sistem, kode sumber aplikasi, dan data transaksi produksi harus memiliki kontrol yang lebih luas untuk mencegah perubahan (misalnya , pemeriksa integrita s, hash kriptografi). Selain itu, kebijakan harus meminimalkan distribusi informasi sensitif, termasuk cetakan yang berisi informasi.	rds-snapshot-encry pted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.10 (b)	b) Informasi sensitif seperti dokumentasi sistem, kode sumber aplikasi, dan data transaksi produksi harus memiliki kontrol yang lebih luas untuk mencegah perubahan (misalnya , pemeriksa integrita s, hash kriptografi). Selain itu, kebijakan harus meminimalkan distribusi informasi sensitif, termasuk cetakan yang berisi informasi.	s3- default-encryption -kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.10 (b)	b) Informasi sensitif seperti dokumentasi sistem, kode sumber aplikasi, dan data transaksi produksi harus memiliki kontrol yang lebih luas untuk mencegah perubahan (misalnya , pemeriksa integrita s, hash kriptografi). Selain itu, kebijakan harus meminimalkan distribusi informasi sensitif, termasuk cetakan yang berisi informasi.	api-gw-cache-enabl ed-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.10 (b)	b) Informasi sensitif seperti dokumentasi sistem, kode sumber aplikasi, dan data transaksi produksi harus memiliki kontrol yang lebih luas untuk mencegah perubahan (misalnya, pemeriksa integritas, hash kriptografi). Selain itu, kebijakan harus meminimalkan distribusi informasi sensitif, termasuk cetakan yang berisi informasi.	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.10 (b)	b) Informasi sensitif seperti dokumentasi sistem, kode sumber aplikasi, dan data transaksi produksi harus memiliki kontrol yang lebih luas untuk mencegah perubahan (misalnya , pemeriksa integrita s, hash kriptografi). Selain itu, kebijakan harus meminimalkan distribusi informasi sensitif, termasuk cetakan yang berisi informasi.	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.10 (b)	b) Informasi sensitif seperti dokumentasi sistem, kode sumber aplikasi, dan data transaksi produksi harus memiliki kontrol yang lebih luas untuk mencegah perubahan (misalnya , pemeriksa integrita s, hash kriptografi). Selain itu, kebijakan harus meminimalkan distribusi informasi sensitif, termasuk cetakan yang berisi informasi.	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.2.1 (h)	h) Untuk meminimal kan risiko yang terkait dengan perubahan, BFIs harus melakukan backup sistem atau aplikasi yang terpengaruh sebelum perubahan. BFIs harus membuat rencana rollback untuk kembali ke versi sebelumnya dari sistem atau aplikasi jika masalah ditemui selama atau setelah penerapan.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.2.1 (h)	h) Untuk meminimalkan risiko yang terkait dengan perubahan, BFIs harus melakukan backup sistem atau aplikasi yang terpengaruh sebelum perubahan. BFIs harus membuat rencana rollback untuk kembali ke versi sebelumnya dari sistem atau aplikasi jika masalah ditemui selama atau setelah penerapan.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.2.1 (h)	h) Untuk meminimalkan risiko yang terkait dengan perubahan, BFIs harus melakukan backup sistem atau aplikasi yang terpengaruh sebelum perubahan. BFIs harus membuat rencana rollback untuk kembali ke versi sebelumnya dari sistem atau aplikasi jika masalah ditemui selama atau setelah penerapan.	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.2.1 (h)	h) Untuk meminimal kan risiko yang terkait dengan perubahan, BFIs harus melakukan backup sistem atau aplikasi yang terpengaruh sebelum perubahan. BFIs harus membuat rencana rollback untuk kembali ke versi sebelumnya dari sistem atau aplikasi jika masalah ditemui selama atau setelah penerapan.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.2.1 (h)	h) Untuk meminimal kan risiko yang terkait dengan perubahan, BFIs harus melakukan backup sistem atau aplikasi yang terpengaruh sebelum perubahan. BFIs harus membuat rencana rollback untuk kembali ke versi sebelumnya dari sistem atau aplikasi jika masalah ditemui selama atau setelah penerapan.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.2.1 (h)	h) Untuk meminimal kan risiko yang terkait dengan perubahan, BFIs harus melakukan backup sistem atau aplikasi yang terpengaruh sebelum perubahan. BFIs harus membuat rencana rollback untuk kembali ke versi sebelumnya dari sistem atau aplikasi jika masalah ditemui selama atau setelah penerapan.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.2.1 (h)	h) Untuk meminimal kan risiko yang terkait dengan perubahan, BFIs harus melakukan backup sistem atau aplikasi yang terpengaruh sebelum perubahan. BFIs harus membuat rencana rollback untuk kembali ke versi sebelumnya dari sistem atau aplikasi jika masalah ditemui selama atau setelah penerapan.	dynamodb-in-backup-plan	Untuk membantu proses pencadang an data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.2.1 (h)	h) Untuk meminimal kan risiko yang terkait dengan perubahan, BFIs harus melakukan backup sistem atau aplikasi yang terpengaruh sebelum perubahan. BFIs harus membuat rencana rollback untuk kembali ke versi sebelumnya dari sistem atau aplikasi jika masalah ditemui selama atau setelah penerapan.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.2.1 (h)	h) Untuk meminimal kan risiko yang terkait dengan perubahan, BFIs harus melakukan backup sistem atau aplikasi yang terpengaruh sebelum perubahan. BFIs harus membuat rencana rollback untuk kembali ke versi sebelumnya dari sistem atau aplikasi jika masalah ditemui selama atau setelah penerapan.	efs-in-backup-plan	Untuk membantu proses pencadang an data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.2.1 (h)	h) Untuk meminimal kan risiko yang terkait dengan perubahan, BFIs harus melakukan backup sistem atau aplikasi yang terpengaruh sebelum perubahan. BFIs harus membuat rencana rollback untuk kembali ke versi sebelumnya dari sistem atau aplikasi jika masalah ditemui selama atau setelah penerapan.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.2.1 (h)	h) Untuk meminimalkan risiko yang terkait dengan perubahan, BFIs harus melakukan backup sistem atau aplikasi yang terpengaruh sebelum perubahan. BFIs harus membuat rencana rollback untuk kembali ke versi sebelumnya dari sistem atau aplikasi jika masalah ditemui selama atau setelah penerapan.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.
3.2.1 (k)	k) Log audit dan keamanan adalah informasi berguna yang memfasilitasi investigasi dan pemecahan masalah. BFI harus memastikan bahwa fasilitas logging diaktifkan untuk merekam kegiatan yang dilakukan selama proses migrasi.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.2.1 (k)	k) Log audit dan keamanan adalah informasi berguna yang memfasili tasi investigasi dan pemecahan masalah. BFI harus memastika n bahwa fasilitas logging diaktifka n untuk merekam kegiatan yang dilakukan selama proses migrasi.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
3.2.1 (k)	k) Log audit dan keamanan adalah informasi berguna yang memfasili tasi investigasi dan pemecahan masalah. BFI harus memastika n bahwa fasilitas logging diaktifka n untuk merekam kegiatan yang dilakukan selama proses migrasi.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.2.1 (k)	k) Log audit dan keamanan adalah informasi berguna yang memfasili tasi investigasi dan pemecahan masalah. BFI harus memastika n bahwa fasilitas logging diaktifka n untuk merekam kegiatan yang dilakukan selama proses migrasi.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteks i aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
3.2.1 (k)	k) Log audit dan keamanan adalah informasi berguna yang memfasili tasi investigasi dan pemecahan masalah. BFI harus memastika n bahwa fasilitas logging diaktifka n untuk merekam kegiatan yang dilakukan selama proses migrasi.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.2.1 (k)	k) Log audit dan keamanan adalah informasi berguna yang memfasili tasi investigasi dan pemecahan masalah. BFI harus memastika n bahwa fasilitas logging diaktifka n untuk merekam kegiatan yang dilakukan selama proses migrasi.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.2.1 (k)	k) Log audit dan keamanan adalah informasi berguna yang memfasili tasi investigasi dan pemecahan masalah. BFI harus memastika n bahwa fasilitas logging diaktifka n untuk merekam kegiatan yang dilakukan selama proses migrasi.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediak an metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinc i untuk permintaa n yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.2.1 (k)	k) Log audit dan keamanan adalah informasi berguna yang memfasili tasi investigasi dan pemecahan masalah. BFI harus memastika n bahwa fasilitas logging diaktifka n untuk merekam kegiatan yang dilakukan selama proses migrasi.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang pergi ke dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
3.2.1 (k)	k) Log audit dan keamanan adalah informasi berguna yang memfasili tasi investigasi dan pemecahan masalah. BFI harus memastika n bahwa fasilitas logging diaktifka n untuk merekam kegiatan yang dilakukan selama proses migrasi.	cw-loggroup-retent ion-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonst ruksi dan mengident ifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.2.1 (k)	k) Log audit dan keamanan adalah informasi berguna yang memfasili tasi investigasi dan pemecahan masalah. BFI harus memastika n bahwa fasilitas logging diaktifka n untuk merekam kegiatan yang dilakukan selama proses migrasi.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.2.1 (k)	k) Log audit dan keamanan adalah informasi berguna yang memfasili tasi investigasi dan pemecahan masalah. BFI harus memastika n bahwa fasilitas logging diaktifka n untuk merekam kegiatan yang dilakukan selama proses migrasi.	wafv2-logging-diak tifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatata n AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.2.1 (k)	k) Log audit dan keamanan adalah informasi berguna yang memfasili tasi investigasi dan pemecahan masalah. BFI harus memastika n bahwa fasilitas logging diaktifka n untuk merekam kegiatan yang dilakukan selama proses migrasi.	redshift-cluster-c onfiguration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastika n bahwa konfigura si yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberika n informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapka n untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.2.1 (k)	k) Log audit dan keamanan adalah informasi berguna yang memfasili tasi investigasi dan pemecahan masalah. BFI harus memastika n bahwa fasilitas logging diaktifka n untuk merekam kegiatan yang dilakukan selama proses migrasi.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.
3.2.1 (k)	k) Log audit dan keamanan adalah informasi berguna yang memfasili tasi investigasi dan pemecahan masalah. BFI harus memastika n bahwa fasilitas logging diaktifka n untuk merekam kegiatan yang dilakukan selama proses migrasi.	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.2.3 (a)	a) Mengembangkan dan menerapka n proses untuk mencegah, mendeteksi, menganalisis, dan menanggapi insiden keamanan informasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.2.3 (a)	a) Mengembangkan dan menerapka n proses untuk mencegah, mendeteksi, menganalisis, dan menanggapi insiden keamanan informasi.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1 (a)	a) Pertimbangkan faktor-faktor penting yang terkait dengan menjaga ketersedi aan sistem yang tinggi, kapasitas yang memadai, kinerja yang andal, waktu respons yang cepat, skalabilitas sebagai bagian dari desain sistem.	dynamodb-autoscali ng-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughpu t yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tuli s yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1 (a)	a) Pertimbangkan faktor-faktor penting yang terkait dengan menjaga ketersedi aan sistem yang tinggi, kapasitas yang memadai, kinerja yang andal, waktu respons yang cepat, skalabilitas sebagai bagian dari desain sistem.	dynamodb-pitr-enab led	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertah ankan cadangan dengan memastika n bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1 (a)	a) Pertimbangkan faktor-faktor penting yang terkait dengan menjaga ketersediaan sistem yang tinggi, kapasitas yang memadai, kinerja yang andal, waktu respons yang cepat, skalabilitas sebagai bagian dari desain sistem.	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.
3.3.1 (a)	a) Pertimbangkan faktor-faktor penting yang terkait dengan menjaga ketersediaan sistem yang tinggi, kapasitas yang memadai, kinerja yang andal, waktu respons yang cepat, skalabilitas sebagai bagian dari desain sistem.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1 (a)	a) Pertimbangkan faktor-faktor penting yang terkait dengan menjaga ketersedi aan sistem yang tinggi, kapasitas yang memadai, kinerja yang andal, waktu respons yang cepat, skalabilitas sebagai bagian dari desain sistem.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersedi aan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplika si data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastru ktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutk an operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1 (a)	a) Pertimbangkan faktor-faktor penting yang terkait dengan menjaga ketersedi aan sistem yang tinggi, kapasitas yang memadai, kinerja yang andal, waktu respons yang cepat, skalabilitas sebagai bagian dari desain sistem.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1 (a)	a) Pertimbangkan faktor-faktor penting yang terkait dengan menjaga ketersedi aan sistem yang tinggi, kapasitas yang memadai, kinerja yang andal, waktu respons yang cepat, skalabilitas sebagai bagian dari desain sistem.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1 (a)	a) Pertimbangkan faktor-faktor penting yang terkait dengan menjaga ketersedi aan sistem yang tinggi, kapasitas yang memadai, kinerja yang andal, waktu respons yang cepat, skalabilitas sebagai bagian dari desain sistem.	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimpleme ntasikan untuk mencapai persyarat an ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivi tas jika salah satu koneksi Site-to-S ite VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivi tas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1 (a)	a) Pertimbangkan faktor-faktor penting yang terkait dengan menjaga ketersedi aan sistem yang tinggi, kapasitas yang memadai, kinerja yang andal, waktu respons yang cepat, skalabilitas sebagai bagian dari desain sistem.	elb-cross-zone-loa d-menyeimbangkan diaktifkan	Aktifkan penyeimba ngan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimba ngan beban lintas zona mengurang i kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkat kan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1 (a)	a) Pertimbangkan faktor-faktor penting yang terkait dengan menjaga ketersedi aan sistem yang tinggi, kapasitas yang memadai, kinerja yang andal, waktu respons yang cepat, skalabilitas sebagai bagian dari desain sistem.	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relationa l Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindun gan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersedi aan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1 (a)	a) Pertimbangkan faktor-faktor penting yang terkait dengan menjaga ketersedi aan sistem yang tinggi, kapasitas yang memadai, kinerja yang andal, waktu respons yang cepat, skalabilitas sebagai bagian dari desain sistem.	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemelihar aan kapasitas dan ketersediaan yang memadai. Penyeimba ng beban secara berkala mengirimk an ping, mencoba koneksi, atau mengirim permintaa n untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scal ing. Jika instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1 (a)	a) Pertimbangkan faktor-faktor penting yang terkait dengan menjaga ketersedi aan sistem yang tinggi, kapasitas yang memadai, kinerja yang andal, waktu respons yang cepat, skalabilitas sebagai bagian dari desain sistem.	dynamodb-throughpu t-limit-check	Aktifkan aturan ini untuk memastika n bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/ tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyarat an throughput Anda. Aturan ini menghasil kan peringatan ketika throughpu t mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentas e WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
3.3.1 (a)	a) Pertimbangkan faktor-faktor penting yang terkait dengan menjaga ketersedi aan sistem yang tinggi, kapasitas yang memadai, kinerja yang andal, waktu respons yang cepat, skalabilitas sebagai bagian dari desain sistem.	lambda-concurrency-check	Aturan ini memastika n bahwa batas tinggi dan rendah konkurens i fungsi Lambda ditetapkan. Ini dapat membantu dalam mendasarkan jumlah permintaan yang dilayani oleh fungsi Anda pada waktu tertentu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (a) (b) (c) (f) (j)	a) Pastikan bahwa catatan akses pengguna diidentif ikasi secara unik dan dicatat untuk tujuan audit dan peninjauan. b) Memiliki akuntabil itas dan identifikasi akses yang tidak sah didokumentasikan. c) Aktifkan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna yang memiliki hak istimewa. f) Memastikan pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat memengaruhi, atau relevan dengan, keamanan informasi. j) Pastikan pencatatan peristiwa menetapka n dasar untuk sistem pemantaua n otomatis yang mampu menghasilkan laporan dan peringata n terkonsolidasi keamanan sistem.	api-gw-execution-l ogging-diaktifkan	Pencatatan API Gateway menampilk an tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (a) (b) (c) (f) (j)	a) Pastikan bahwa catatan akses pengguna diidentif ikasi secara unik dan dicatat untuk tujuan audit dan peninjauan. b) Memiliki akuntabil itas dan identifikasi akses yang tidak sah didokumentasikan. c) Aktifkan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna yang memiliki hak istimewa. f) Memastikan pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat memengaruhi, atau relevan dengan, keamanan informasi. j) Pastikan pencatatan peristiwa menetapka n dasar untuk sistem pemantaua n otomatis yang mampu menghasilkan laporan dan peringata n terkonsolidasi keamanan sistem.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (a) (b) (c) (f) (j)	a) Pastikan bahwa catatan akses pengguna diidentif ikasi secara unik dan dicatat untuk tujuan audit dan peninjauan. b) Memiliki akuntabil itas dan identifikasi akses yang tidak sah didokumentasikan. c) Aktifkan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna yang memiliki hak istimewa. f) Memastikan pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat memengaruhi, atau relevan dengan, keamanan informasi. j) Pastikan pencatatan peristiwa menetapka n dasar untuk sistem pemantaua n otomatis yang mampu menghasilkan laporan dan peringata n terkonsolidasi keamanan sistem.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (a) (b) (c) (f) (j)	a) Pastikan bahwa catatan akses pengguna diidentif ikasi secara unik dan dicatat untuk tujuan audit dan peninjauan. b) Memiliki akuntabil itas dan identifikasi akses yang tidak sah didokumentasikan. c) Aktifkan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna yang memiliki hak istimewa. f) Memastikan pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat memengaruhi, atau relevan dengan, keamanan informasi. j) Pastikan pencatatan peristiwa menetapka n dasar untuk sistem pemantaua n otomatis yang mampu menghasilkan laporan dan peringata n terkonsolidasi keamanan sistem.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteks i aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (a) (b) (c) (f) (j)	a) Pastikan bahwa catatan akses pengguna diidentif ikasi secara unik dan dicatat untuk tujuan audit dan peninjauan. b) Memiliki akuntabil itas dan identifikasi akses yang tidak sah didokumentasikan. c) Aktifkan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna yang memiliki hak istimewa. f) Memastikan pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat memengaruhi, atau relevan dengan, keamanan informasi. j) Pastikan pencatatan peristiwa menetapka n dasar untuk sistem pemantaua n otomatis yang mampu menghasilkan laporan dan peringata n terkonsolidasi keamanan sistem.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus, atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (a) (b) (c) (f) (j)	a) Pastikan bahwa catatan akses pengguna diidentif ikasi secara unik dan dicatat untuk tujuan audit dan peninjauan. b) Memiliki akuntabil itas dan identifikasi akses yang tidak sah didokumentasikan. c) Aktifkan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna yang memiliki hak istimewa. f) Memastikan pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat memengaruhi, atau relevan dengan, keamanan informasi. j) Pastikan pencatatan peristiwa menetapka n dasar untuk sistem pemantaua n otomatis yang mampu menghasilkan laporan dan peringata n terkonsolidasi keamanan sistem.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (a) (b) (c) (f) (j)	a) Pastikan bahwa catatan akses pengguna diidentif ikasi secara unik dan dicatat untuk tujuan audit dan peninjauan. b) Memiliki akuntabil itas dan identifikasi akses yang tidak sah didokumentasikan. c) Aktifkan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna yang memiliki hak istimewa. f) Memastikan pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat memengaruhi, atau relevan dengan, keamanan informasi. j) Pastikan pencatatan peristiwa menetapka n dasar untuk sistem pemantaua n otomatis yang mampu menghasilkan laporan dan peringata n terkonsolidasi keamanan sistem.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (a) (b) (c) (f) (j)	a) Pastikan bahwa catatan akses pengguna diidentif ikasi secara unik dan dicatat untuk tujuan audit dan peninjauan. b) Memiliki akuntabil itas dan identifikasi akses yang tidak sah didokumentasikan. c) Aktifkan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna yang memiliki hak istimewa. f) Memastikan pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat memengaruhi, atau relevan dengan, keamanan informasi. j) Pastikan pencatatan peristiwa menetapka n dasar untuk sistem pemantaua n otomatis yang mampu menghasilkan laporan dan peringata n terkonsolidasi keamanan sistem.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediak an metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinc i untuk permintaa n yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (a) (b) (c) (f) (j)	a) Pastikan bahwa catatan akses pengguna diidentif ikasi secara unik dan dicatat untuk tujuan audit dan peninjauan. b) Memiliki akuntabil itas dan identifikasi akses yang tidak sah didokumentasikan. c) Aktifkan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna yang memiliki hak istimewa. f) Memastikan pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat memengaruhi, atau relevan dengan, keamanan informasi. j) Pastikan pencatatan peristiwa menetapka n dasar untuk sistem pemantaua n otomatis yang mampu menghasilkan laporan dan peringata n terkonsolidasi keamanan sistem.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang pergi ke dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (a) (b) (c) (f) (j)	a) Pastikan bahwa catatan akses pengguna diidentif ikasi secara unik dan dicatat untuk tujuan audit dan peninjauan. b) Memiliki akuntabil itas dan identifikasi akses yang tidak sah didokumentasikan. c) Aktifkan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna yang memiliki hak istimewa. f) Memastikan pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat memengaruhi, atau relevan dengan, keamanan informasi. j) Pastikan pencatatan peristiwa menetapka n dasar untuk sistem pemantaua n otomatis yang mampu menghasilkan laporan dan peringata n terkonsolidasi keamanan sistem.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (a) (b) (c) (f) (j)	a) Pastikan bahwa catatan akses pengguna diidentif ikasi secara unik dan dicatat untuk tujuan audit dan peninjauan. b) Memiliki akuntabil itas dan identifikasi akses yang tidak sah didokumentasikan. c) Aktifkan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna yang memiliki hak istimewa. f) Memastikan pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat memengaruhi, atau relevan dengan, keamanan informasi. j) Pastikan pencatatan peristiwa menetapka n dasar untuk sistem pemantaua n otomatis yang mampu menghasilkan laporan dan peringata n terkonsolidasi keamanan sistem.	wafv2-logging-diak tifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatata n AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (a) (b) (c) (f) (j)	a) Pastikan bahwa catatan akses pengguna diidentif ikasi secara unik dan dicatat untuk tujuan audit dan peninjauan. b) Memiliki akuntabil itas dan identifikasi akses yang tidak sah didokumentasikan. c) Aktifkan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna yang memiliki hak istimewa. f) Memastikan pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat memengaruhi, atau relevan dengan, keamanan informasi. j) Pastikan pencatatan peristiwa menetapka n dasar untuk sistem pemantaua n otomatis yang mampu menghasilkan laporan dan peringata n terkonsolidasi keamanan sistem.	redshift-cluster-c onfiguration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastika n bahwa konfigura si yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberika n informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapka n untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (a) (b) (c) (f) (j)	a) Pastikan bahwa catatan akses pengguna diidentif ikasi secara unik dan dicatat untuk tujuan audit dan peninjauan. b) Memiliki akuntabil itas dan identifikasi akses yang tidak sah didokumentasikan. c) Aktifkan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna yang memiliki hak istimewa. f) Memastikan pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat memengaruhi, atau relevan dengan, keamanan informasi. j) Pastikan pencatatan peristiwa menetapka n dasar untuk sistem pemantaua n otomatis yang mampu menghasilkan laporan dan peringata n terkonsolidasi keamanan sistem.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (a) (b) (c) (f) (j)	a) Pastikan bahwa catatan akses pengguna diidentif ikasi secara unik dan dicatat untuk tujuan audit dan peninjauan. b) Memiliki akuntabil itas dan identifikasi akses yang tidak sah didokumentasikan. c) Aktifkan pencatatan audit aktivitas sistem yang dilakukan oleh pengguna yang memiliki hak istimewa. f) Memastikan pencatatan dan pemantauan yang tepat harus diterapka n untuk memungkin kan pencatatan dan deteksi tindakan yang dapat memengaruhi, atau relevan dengan, keamanan informasi. j) Pastikan pencatatan peristiwa menetapka n dasar untuk sistem pemantaua n otomatis yang mampu menghasilkan laporan dan peringata n terkonsolidasi keamanan sistem.	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (f)	f) Memastikan pencatatan dan pemantauan yang tepat harus diterapkan untuk memungkinkan pencatatan dan deteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan informasi.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (g)	g) Pastikan log peristiwa mencakup, bila relevan: - Pengguna IDs - Aktivitas sistem - Tanggal, waktu, dan detail peristiwa penting, misalnya log-on dan log-off - Identitas perangkat atau lokasi jika memungkinkan dan pengidentifikasi sistem - Catatan upaya akses sistem yang berhasil dan ditolak - Catatan data yang berhasil dan ditolak dan upaya akses sumber daya lainnya - Perubahan konfigurasi sistem - Penggunaan hak istimewa - Penggunaan utilitas dan aplikasi sistem - File yang diakses dan jenis akses - Alamat jaringan dan protokol - Alarm dinaikkan oleh kontrol akses sistem dan - Catatan transaksi yang dijalankan oleh	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	pengguna dalam aplikasi dan transaksi pelanggan online		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (g)	g) Pastikan log peristiwa mencakup, bila relevan: - Pengguna IDs - Aktivitas sistem - Tanggal, waktu, dan detail peristiwa penting, misalnya log-on dan log-off - Identitas perangkat atau lokasi jika memungkinkan dan pengidentifikasi sistem - Catatan upaya akses sistem yang berhasil dan ditolak - Catatan data yang berhasil dan ditolak dan upaya akses sumber daya lainnya - Perubahan konfigurasi sistem - Penggunaan hak istimewa - Penggunaan utilitas dan aplikasi sistem - File yang diakses dan jenis akses - Alamat jaringan dan protokol - Alarm dinaikkan oleh kontrol akses sistem dan - Catatan transaksi yang dijalankan oleh	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	pengguna dalam aplikasi dan transaksi pelanggan online		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (g)	g) Pastikan log peristiwa mencakup, bila relevan: - Pengguna IDs - Aktivitas sistem - Tanggal, waktu, dan detail peristiwa penting, misalnya log-on dan log-off - Identitas perangkat atau lokasi jika memungkinkan dan pengidentifikasi sistem - Catatan upaya akses sistem yang berhasil dan ditolak - Catatan data yang berhasil dan ditolak dan upaya akses sumber daya lainnya - Perubahan konfigurasi sistem - Penggunaan hak istimewa - Penggunaan utilitas dan aplikasi sistem - File yang diakses dan jenis akses - Alamat jaringan dan protokol - Alarm dinaikkan oleh kontrol akses sistem dan - Catatan transaksi yang dijalankan oleh	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	pengguna dalam aplikasi dan transaksi pelanggan online		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (g)	g) Pastikan log peristiwa mencakup, bila relevan: - Pengguna IDs - Aktivitas sistem - Tanggal, waktu, dan detail peristiwa penting, misalnya log-on dan log-off - Identitas perangkat atau lokasi jika memungkinkan dan pengidentifikasi sistem - Catatan upaya akses sistem yang berhasil dan ditolak - Catatan data yang berhasil dan ditolak dan upaya akses sumber daya lainnya - Perubahan konfigurasi sistem - Penggunaan hak istimewa - Penggunaan utilitas dan aplikasi sistem - File yang diakses dan jenis akses - Alamat jaringan dan protokol - Alarm dinaikkan oleh kontrol akses sistem dan - Catatan transaksi yang dijalankan oleh	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	pengguna dalam aplikasi dan transaksi pelanggan online		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (g)	g) Pastikan log peristiwa mencakup, bila relevan: - Pengguna IDs - Aktivitas sistem - Tanggal, waktu, dan detail peristiwa penting, misalnya log-on dan log-off - Identitas perangkat atau lokasi jika memungkinkan dan pengidentifikasi sistem - Catatan upaya akses sistem yang berhasil dan ditolak - Catatan data yang berhasil dan ditolak dan upaya akses sumber daya lainnya - Perubahan konfigurasi sistem - Penggunaan hak istimewa - Penggunaan utilitas dan aplikasi sistem - File yang diakses dan jenis akses - Alamat jaringan dan protokol - Alarm dinaikkan oleh kontrol akses sistem dan - Catatan transaksi yang dijalankan oleh	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	pengguna dalam aplikasi dan transaksi pelanggan online		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (g)	g) Pastikan log peristiwa mencakup, bila relevan: - Pengguna IDs - Aktivitas sistem - Tanggal, waktu, dan detail peristiwa penting, misalnya log-on dan log-off - Identitas perangkat atau lokasi jika memungkinkan dan pengidentifikasi sistem - Catatan upaya akses sistem yang berhasil dan ditolak - Catatan data yang berhasil dan ditolak dan upaya akses sumber daya lainnya - Perubahan konfigurasi sistem - Penggunaan hak istimewa - Penggunaan utilitas dan aplikasi sistem - File yang diakses dan jenis akses - Alamat jaringan dan protokol - Alarm dinaikkan oleh kontrol akses sistem dan - Catatan transaksi yang dijalankan oleh	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	pengguna dalam aplikasi dan transaksi pelanggan online		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (g)	g) Pastikan log peristiwa mencakup, bila relevan: - Pengguna IDs - Aktivitas sistem - Tanggal, waktu, dan detail peristiwa penting, misalnya log-on dan log-off - Identitas perangkat atau lokasi jika memungkinkan dan pengidentifikasi sistem - Catatan upaya akses sistem yang berhasil dan ditolak - Catatan data yang berhasil dan ditolak dan upaya akses sumber daya lainnya - Perubahan konfigurasi sistem - Penggunaan hak istimewa - Penggunaan utilitas dan aplikasi sistem - File yang diakses dan jenis akses - Alamat jaringan dan protokol - Alarm dinaikkan oleh kontrol akses sistem dan - Catatan transaksi yang dijalankan oleh	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	pengguna dalam aplikasi dan transaksi pelanggan online		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (g)	g) Pastikan log peristiwa mencakup, bila relevan: - Pengguna IDs - Aktivitas sistem - Tanggal, waktu, dan detail peristiwa penting, misalnya log-on dan log-off - Identitas perangkat atau lokasi jika memungkinkan dan pengidentifikasi sistem - Catatan upaya akses sistem yang berhasil dan ditolak - Catatan data yang berhasil dan ditolak dan upaya akses sumber daya lainnya - Perubahan konfigurasi sistem - Penggunaan hak istimewa - Penggunaan utilitas dan aplikasi sistem - File yang diakses dan jenis akses - Alamat jaringan dan protokol - Alarm dinaikkan oleh kontrol akses sistem dan - Catatan transaksi yang dijalankan oleh	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	pengguna dalam aplikasi dan transaksi pelanggan online		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (g)	g) Pastikan log peristiwa mencakup, bila relevan: - Pengguna IDs - Aktivitas sistem - Tanggal, waktu, dan detail peristiwa penting, misalnya log-on dan log-off - Identitas perangkat atau lokasi jika memungkinkan dan pengidentifikasi sistem - Catatan upaya akses sistem yang berhasil dan ditolak - Catatan data yang berhasil dan ditolak dan upaya akses sumber daya lainnya - Perubahan konfigurasi sistem - Penggunaan hak istimewa - Penggunaan utilitas dan aplikasi sistem - File yang diakses dan jenis akses - Alamat jaringan dan protokol - Alarm dinaikkan oleh kontrol akses sistem dan - Catatan transaksi yang dijalankan oleh	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	pengguna dalam aplikasi dan transaksi pelanggan online		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (g)	g) Pastikan log peristiwa mencakup, bila relevan: - Pengguna IDs - Aktivitas sistem - Tanggal, waktu, dan detail peristiwa penting, misalnya log-on dan log-off - Identitas perangkat atau lokasi jika memungkinkan dan pengidentifikasi sistem - Catatan upaya akses sistem yang berhasil dan ditolak - Catatan data yang berhasil dan ditolak dan upaya akses sumber daya lainnya - Perubahan konfigurasi sistem - Penggunaan hak istimewa - Penggunaan utilitas dan aplikasi sistem - File yang diakses dan jenis akses - Alamat jaringan dan protokol - Alarm dinaikkan oleh kontrol akses sistem dan - Catatan transaksi yang dijalankan oleh	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	pengguna dalam aplikasi dan transaksi pelanggan online		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (g)	g) Pastikan log peristiwa mencakup, bila relevan: - Pengguna IDs - Aktivitas sistem - Tanggal, waktu, dan detail peristiwa penting, misalnya log-on dan log-off - Identitas perangkat atau lokasi jika memungkinkan dan pengidentifikasi sistem - Catatan upaya akses sistem yang berhasil dan ditolak - Catatan data yang berhasil dan ditolak dan upaya akses sumber daya lainnya - Perubahan konfigurasi sistem - Penggunaan hak istimewa - Penggunaan utilitas dan aplikasi sistem - File yang diakses dan jenis akses - Alamat jaringan dan protokol - Alarm dinaikkan oleh kontrol akses sistem dan - Catatan transaksi yang dijalankan oleh	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang pergi ke dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	pengguna dalam aplikasi dan transaksi pelanggan online		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (g)	g) Pastikan log peristiwa mencakup, bila relevan: - Pengguna IDs - Aktivitas sistem - Tanggal, waktu, dan detail peristiwa penting, misalnya log-on dan log-off - Identitas perangkat atau lokasi jika memungkinkan dan pengidentifikasi sistem - Catatan upaya akses sistem yang berhasil dan ditolak - Catatan data yang berhasil dan ditolak dan upaya akses sumber daya lainnya - Perubahan konfigurasi sistem - Penggunaan hak istimewa - Penggunaan utilitas dan aplikasi sistem - File yang diakses dan jenis akses - Alamat jaringan dan protokol - Alarm dinaikkan oleh kontrol akses sistem dan - Catatan transaksi yang dijalankan oleh	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	pengguna dalam aplikasi dan transaksi pelanggan online		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (g)	g) Pastikan log peristiwa mencakup, bila relevan: - Pengguna IDs - Aktivitas sistem - Tanggal, waktu, dan detail peristiwa penting, misalnya log-on dan log-off - Identitas perangkat atau lokasi jika memungkinkan dan pengidentifikasi sistem - Catatan upaya akses sistem yang berhasil dan ditolak - Catatan data yang berhasil dan ditolak dan upaya akses sumber daya lainnya - Perubahan konfigurasi sistem - Penggunaan hak istimewa - Penggunaan utilitas dan aplikasi sistem - File yang diakses dan jenis akses - Alamat jaringan dan protokol - Alarm dinaikkan oleh kontrol akses sistem dan - Catatan transaksi yang dijalankan oleh	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	pengguna dalam aplikasi dan transaksi pelanggan online		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4 (g)	g) Pastikan log peristiwa mencakup, bila relevan: - Pengguna IDs - Aktivitas sistem - Tanggal, waktu, dan detail peristiwa penting, misalnya log-on dan log-off - Identitas perangkat atau lokasi jika memungkinkan dan pengidentifikasi sistem - Catatan upaya akses sistem yang berhasil dan ditolak - Catatan data yang berhasil dan ditolak dan upaya akses sumber daya lainnya - Perubahan konfigurasi sistem - Penggunaan hak istimewa - Penggunaan utilitas dan aplikasi sistem - File yang diakses dan jenis akses - Alamat jaringan dan protokol - Alarm dinaikkan oleh kontrol akses sistem dan - Catatan transaksi yang dijalankan oleh	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	pengguna dalam aplikasi dan transaksi pelanggan online		
3.6.1 (a) (h)	a) BFIs perlu memastikan langkah-langkah keamanan yang sesuai untuk aplikasi web mereka dan mengambil langkah-langkah mitigasi yang wajar terhadap berbagai risiko keamanan web. h) BFIs perlu memastikan langkah-langkah keamanan yang sesuai untuk aplikasi web mereka dan mengambil langkah-langkah mitigasi yang wajar terhadap berbagai risiko keamanan web	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.1 (a) (h)	a) BFIs perlu memastikan langkah-langkah keamanan yang sesuai untuk aplikasi web mereka dan mengambil langkah-langkah mitigasi yang wajar terhadap berbagai risiko keamanan web. h) BFIs perlu memastikan langkah-langkah keamanan yang sesuai untuk aplikasi web mereka dan mengambil langkah-langkah mitigasi yang wajar terhadap berbagai risiko keamanan web	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindungnya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.1 (b)	b) BFIs perlu mengevaluasi persyaratan keamanan yang terkait dengan sistem perbankan internet mereka dan sistem lain yang relevan dan mengadopsi solusi enkripsi dengan mempertimbangkan tingkat kerahasiaan dan integritas yang diperlukan.	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.
3.6.1 (b)	b) BFIs perlu mengevaluasi persyaratan keamanan yang terkait dengan sistem perbankan internet mereka dan sistem lain yang relevan dan mengadopsi solusi enkripsi dengan mempertimbangkan tingkat kerahasiaan dan integritas yang diperlukan.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.1 (b)	b) BFIs perlu mengevaluasi persyaratan keamanan yang terkait dengan sistem perbankan internet mereka dan sistem lain yang relevan dan mengadopsi solusi enkripsi dengan mempertimbangkan tingkat kerahasiaan dan integritas yang diperlukan.	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
3.6.1 (b)	b) BFIs perlu mengevaluasi persyaratan keamanan yang terkait dengan sistem perbankan internet mereka dan sistem lain yang relevan dan mengadopsi solusi enkripsi dengan mempertimbangkan tingkat kerahasiaan dan integritas yang diperlukan.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.1 (b)	b) BFIs perlu mengevaluasi persyaratan keamanan yang terkait dengan sistem perbankan internet mereka dan sistem lain yang relevan dan mengadopsi solusi enkripsi dengan mempertimbangkan tingkat kerahasiaan dan integritas yang diperlukan.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
3.6.1 (b)	b) BFIs perlu mengevaluasi persyaratan keamanan yang terkait dengan sistem perbankan internet mereka dan sistem lain yang relevan dan mengadopsi solusi enkripsi dengan mempertimbangkan tingkat kerahasiaan dan integritas yang diperlukan.	alb-http-drop-invalid-header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.1 (b)	b) BFIs perlu mengevaluasi persyaratan keamanan yang terkait dengan sistem perbankan internet mereka dan sistem lain yang relevan dan mengadopsi solusi enkripsi dengan mempertimbangkan tingkat kerahasiaan dan integritas yang diperlukan.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.1 (b)	b) BFIs perlu mengevaluasi persyaratan keamanan yang terkait dengan sistem perbankan internet mereka dan sistem lain yang relevan dan mengadopsi solusi enkripsi dengan mempertimbangkan tingkat kerahasiaan dan integritas yang diperlukan.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
3.6.1 (b)	b) BFIs perlu mengevaluasi persyaratan keamanan yang terkait dengan sistem perbankan internet mereka dan sistem lain yang relevan dan mengadopsi solusi enkripsi dengan mempertimbangkan tingkat kerahasiaan dan integritas yang diperlukan.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.1 (b)	b) BFIs perlu mengevaluasi persyaratan keamanan yang terkait dengan sistem perbankan internet mereka dan sistem lain yang relevan dan mengadopsi solusi enkripsi dengan mempertimbangkan tingkat kerahasiaan dan integritas yang diperlukan.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
3.6.1 (b)	b) BFIs perlu mengevaluasi persyaratan keamanan yang terkait dengan sistem perbankan internet mereka dan sistem lain yang relevan dan mengadopsi solusi enkripsi dengan mempertimbangkan tingkat kerahasiaan dan integritas yang diperlukan.	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.1 (d)	d) BFIs menyediakan internet banking harus responsif terhadap kondisi lalu lintas jaringan/kinerja sistem yang tidak biasa dan lonjakan tiba-tiba dalam pemanfaatan sumber daya sistem yang dapat menjadi indikasi serangan S. DDo Akibatnya , keberhasilan setiap tindakan pre-emptive dan reaktif tergantung pada penyebaran alat yang tepat untuk secara efektif mendeteks i, memantau dan menganalisis anomali dalam jaringan dan sistem.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.1 (d)	d) BFIs menyediakan internet banking harus responsif terhadap kondisi lalu lintas jaringan/kinerja sistem yang tidak biasa dan lonjakan tiba-tiba dalam pemanfaatan sumber daya sistem yang dapat menjadi indikasi serangan S. DDo Akibatnya , keberhasilan setiap tindakan pre-emptive dan reaktif tergantung pada penyebaran alat yang tepat untuk secara efektif mendeteks i, memantau dan menganalisis anomali dalam jaringan dan sistem.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.1 (d)	d) BFIs menyediakan internet banking harus responsif terhadap kondisi lalu lintas jaringan/kinerja sistem yang tidak biasa dan lonjakan tiba-tiba dalam pemanfaatan sumber daya sistem yang dapat menjadi indikasi serangan S. DDo Akibatnya , keberhasilan setiap tindakan pre-emptive dan reaktif tergantung pada penyebaran alat yang tepat untuk secara efektif mendeteks i, memantau dan menganalisis anomali dalam jaringan dan sistem.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.1 (d)	d) BFIs menyediakan internet banking harus responsif terhadap kondisi lalu lintas jaringan/kinerja sistem yang tidak biasa dan lonjakan tiba-tiba dalam pemanfaatan sumber daya sistem yang dapat menjadi indikasi serangan S. DDo Akibatnya , keberhasilan setiap tindakan pre-emptive dan reaktif tergantung pada penyebaran alat yang tepat untuk secara efektif mendeteks i, memantau dan menganalisis anomali dalam jaringan dan sistem.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatata n AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.1 (d)	d) BFIs menyediakan internet banking harus responsif terhadap kondisi lalu lintas jaringan/kinerja sistem yang tidak biasa dan lonjakan tiba-tiba dalam pemanfaatan sumber daya sistem yang dapat menjadi indikasi serangan S. DDo Akibatnya , keberhasilan setiap tindakan pre-emptive dan reaktif tergantung pada penyebaran alat yang tepat untuk secara efektif mendeteks i, memantau dan menganalisis anomali dalam jaringan dan sistem.	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizink an, memblokir, atau menghitung permintaa n web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindung inya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.1 (e)	e) BFIs perlu secara teratur menilai kerentanan keamanan informasi dan mengevaluasi efektivitas kerangka kerja manajemen risiko keamanan TI yang ada, membuat penyesuaian yang diperlukan untuk memastikan kerentanan yang muncul ditangani tepat waktu. Penilaian ini juga harus dilakukan sebagai bagian dari setiap perubahan material.	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.4 (a) (b)	a) Batasi akses internet & pisahkan sistem kritis dari lingkungan TI Umum. b) Mengurangi permukaan serangan dan kerentanan.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.6.4 (a) (b)	a) Batasi akses internet & pisahkan sistem kritis dari lingkungan TI Umum. b) Mengurangi permukaan serangan dan kerentanan.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.6.4 (a) (b)	a) Batasi akses internet & pisahkan sistem kritis dari lingkungan TI Umum. b) Mengurangi permukaan serangan dan kerentanan.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.4 (a) (b)	a) Batasi akses internet & pisahkan sistem kritis dari lingkungan TI Umum. b) Mengurangi permukaan serangan dan kerentanan.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.4 (a) (b)	a) Batasi akses internet & pisahkan sistem kritis dari lingkungan TI Umum. b) Mengurangi permukaan serangan dan kerentanan.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.4 (a) (b)	a) Batasi akses internet & pisahkan sistem kritis dari lingkungan TI Umum. b) Mengurangi permukaan serangan dan kerentanan.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.6.4 (a) (b)	a) Batasi akses internet & pisahkan sistem kritis dari lingkungan TI Umum. b) Mengurangi permukaan serangan dan kerentanan.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.4 (a) (b)	a) Batasi akses internet & pisahkan sistem kritis dari lingkungan TI Umum. b) Mengurangi permukaan serangan dan kerentanan.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.4 (a) (b)	a) Batasi akses internet & pisahkan sistem kritis dari lingkungan TI Umum. b) Mengurangi permukaan serangan dan kerentanan.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
3.6.4 (a) (b)	a) Batasi akses internet & pisahkan sistem kritis dari lingkungan TI Umum. b) Mengurangi permukaan serangan dan kerentanan.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.4 (a) (b)	a) Batasi akses internet & pisahkan sistem kritis dari lingkungan TI Umum. b) Mengurangi permukaan serangan dan kerentanan.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.4 (a) (b)	a) Batasi akses internet & pisahkan sistem kritis dari lingkungan TI Umum. b) Mengurangi permukaan serangan dan kerentanan.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
3.6.4 (a) (b)	a) Batasi akses internet & pisahkan sistem kritis dari lingkungan TI Umum. b) Mengurangi permukaan serangan dan kerentanan.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.4 (a) (b)	a) Batasi akses internet & pisahkan sistem kritis dari lingkungan TI Umum. b) Mengurangi permukaan serangan dan kerentanan.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.4 (a) (b)	a) Batasi akses internet & pisahkan sistem kritis dari lingkungan TI Umum. b) Mengurangi permukaan serangan dan kerentanan.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.4 (a) (b)	a) Batasi akses internet & pisahkan sistem kritis dari lingkungan TI Umum. b) Mengurangi permukaan serangan dan kerentanan.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
3.6.4 (a) (b)	a) Batasi akses internet & pisahkan sistem kritis dari lingkungan TI Umum. b) Mengurangi permukaan serangan dan kerentanan.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.4 (a) (b)	a) Batasi akses internet & pisahkan sistem kritis dari lingkungan TI Umum. b) Mengurangi permukaan serangan dan kerentanan.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.4 (a) (b)	a) Batasi akses internet & pisahkan sistem kritis dari lingkungan TI Umum. b) Mengurangi permukaan serangan dan kerentanan.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.4 (a) (b)	a) Batasi akses internet & pisahkan sistem kritis dari lingkungan TI Umum. b) Mengurangi permukaan serangan dan kerentanan.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.4 (a) (b)	a) Batasi akses internet & pisahkan sistem kritis dari lingkungan TI Umum. b) Mengurangi permukaan serangan dan kerentanan.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
3.6.4 (a) (b)	a) Batasi akses internet & pisahkan sistem kritis dari lingkungan TI Umum. b) Mengurangi permukaan serangan dan kerentanan.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.4 (a) (b)	a) Batasi akses internet & pisahkan sistem kritis dari lingkungan TI Umum. b) Mengurangi permukaan serangan dan kerentanan.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.4 (a) (b)	a) Batasi akses internet & pisahkan sistem kritis dari lingkungan TI Umum. b) Mengurangi permukaan serangan dan kerentanan.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.4 (a) (b)	a) Batasi akses internet & pisahkan sistem kritis dari lingkungan TI Umum. b) Mengurangi permukaan serangan dan kerentanan.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk NBC TRMG.

Praktik Terbaik Operasional untuk NERC CIP BCSI

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara North American Electric Reliability Corporation Critical Infrastructure Protection Standards (NERC CIP) untuk BES Cyber System Information (BCSI), CIP-004-7 & CIP-011-3, dan aturan terkelola. AWS Config Setiap aturan AWS Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau beberapa kontrol CIP NERC yang berlaku untuk BCSI. Kontrol CIP NERC dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-004-7-R6-Bagian 6.1	Setiap Entitas yang Bertanggung Jawab harus menerapka n satu atau lebih program manajemen akses terdokume ntasi untuk mengotori sasi, memverifikasi, dan mencabut akses yang disediakan ke BCSI yang berkaitan dengan “Sistem yang Berlaku” yang diidentifikasi dalam CIP-004-7 Tabel R6 — Manajemen Akses untuk Informasi Sistem Cyber BES yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-004-7 Tabel R6 — Manajemen Akses untuk Informasi Sistem Cyber BES. Untuk dipertimb angkan akses ke BCSI dalam konteks persyaratan ini, seorang individu memiliki kemampuan untuk memperoleh	opensearch-access-control-enabled	Pastikan kontrol akses berbutir halus diaktifkan di domain Layanan Amazon OpenSearch Anda. Kontrol akses berbutir halus menyediakan mekanisme otorisasi yang disempurn akan untuk mencapai akses yang paling tidak memiliki hak istimewa ke domain Amazon. OpenSearc h Ini memungkin kan kontrol akses berbasis peran ke domain, serta indeks, dokumen, dan keamanan tingkat lapangan, dukungan untuk OpenSearch dasbor multi-tenancy, dan otentikasi dasar HTTP untuk dan Kibana. OpenSearch

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
	dan menggunakan BCSI. Akses yang disediakan harus dianggap sebagai hasil dari tindakan spesifik yang diambil untuk menyediakan sarana bagi individu untuk mengakses BCSI (misalnya, dapat mencakup kunci fisik atau kartu akses, pengguna dan hak dan hak istimewa terkait, kunci enkripsi). Bagian 6.1: Sebelum penyediaa n, otorisasi (kecuali telah diizinkan sesuai dengan Bagian 4.1.) berdasark an kebutuhan , sebagaimana ditentukan oleh Entitas yang Bertanggung Jawab, kecuali untuk Keadaan Luar Biasa CIP: 6.1.1. Akses elektronik yang disediakan ke BCSI elektronik		

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-004-7-R6-Bagian 6.1	Setiap Entitas yang Bertanggung Jawab harus menerapkan satu atau lebih program manajemen akses terdokumentasi untuk mengotorisasi, memverifikasi, dan mencabut akses yang disediakan ke BCSI yang berkaitan dengan “Sistem yang Berlaku” yang diidentifikasi dalam CIP-004-7 Tabel R6 — Manajemen Akses untuk Informasi Sistem Cyber BES yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-004-7 Tabel R6 — Manajemen Akses untuk Informasi Sistem Cyber BES. Untuk dipertimbangkan akses ke BCSI dalam konteks persyaratan ini, seorang individu memiliki kemampuan untuk memperoleh	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktifkan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediakan sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
	dan menggunakan BCSI. Akses yang disediakan harus dianggap sebagai hasil dari tindakan spesifik yang diambil untuk menyediakan sarana bagi individu untuk mengakses BCSI (misalnya, dapat mencakup kunci fisik atau kartu akses, pengguna dan hak dan hak istimewa terkait, kunci enkripsi). Bagian 6.1: Sebelum penyediaa n, otorisasi (kecuali telah diizinkan sesuai dengan Bagian 4.1.) berdasark an kebutuhan , sebagaimana ditentukan oleh Entitas yang Bertanggung Jawab, kecuali untuk Keadaan Luar Biasa CIP: 6.1.1. Akses elektronik yang disediakan ke BCSI elektronik		

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-004-7-R6-Bagian 6.1	Setiap Entitas yang Bertanggung Jawab harus menerapkan satu atau lebih program manajemen akses terdokumentasi untuk mengotorisasi, memverifikasi, dan mencabut akses yang disediakan ke BCSI yang berkaitan dengan “Sistem yang Berlaku” yang diidentifikasi dalam CIP-004-7 Tabel R6 — Manajemen Akses untuk Informasi Sistem Cyber BES yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-004-7 Tabel R6 — Manajemen Akses untuk Informasi Sistem Cyber BES. Untuk dipertimbangkan akses ke BCSI dalam konteks persyaratan ini, seorang individu memiliki kemampuan untuk memperoleh	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
	dan menggunakan BCSI. Akses yang disediakan harus dianggap sebagai hasil dari tindakan spesifik yang diambil untuk menyediakan sarana bagi individu untuk mengakses BCSI (misalnya, dapat mencakup kunci fisik atau kartu akses, pengguna dan hak dan hak istimewa terkait, kunci enkripsi). Bagian 6.1: Sebelum penyediaa n, otorisasi (kecuali telah diizinkan sesuai dengan Bagian 4.1.) berdasark an kebutuhan , sebagaimana ditentukan oleh Entitas yang Bertanggung Jawab, kecuali untuk Keadaan Luar Biasa CIP: 6.1.1. Akses elektronik yang disediakan ke BCSI elektronik		

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-004-7-R6-Bagian 6.1	Setiap Entitas yang Bertanggung Jawab harus menerapkan satu atau lebih program manajemen akses terdokumentasi untuk mengotorisasi, memverifikasi, dan mencabut akses yang disediakan ke BCSI yang berkaitan dengan “Sistem yang Berlaku” yang diidentifikasi dalam CIP-004-7 Tabel R6 — Manajemen Akses untuk Informasi Sistem Cyber BES yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-004-7 Tabel R6 — Manajemen Akses untuk Informasi Sistem Cyber BES. Untuk dipertimbangkan akses ke BCSI dalam konteks persyaratan ini, seorang individu memiliki kemampuan untuk memperoleh	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
	dan menggunakan BCSI. Akses yang disediakan harus dianggap sebagai hasil dari tindakan spesifik yang diambil untuk menyediakan sarana bagi individu untuk mengakses BCSI (misalnya, dapat mencakup kunci fisik atau kartu akses, pengguna dan hak dan hak istimewa terkait, kunci enkripsi). Bagian 6.1: Sebelum penyediaa n, otorisasi (kecuali telah diizinkan sesuai dengan Bagian 4.1.) berdasark an kebutuhan , sebagaimana ditentukan oleh Entitas yang Bertanggung Jawab, kecuali untuk Keadaan Luar Biasa CIP: 6.1.1. Akses elektronik yang disediakan ke BCSI elektronik		

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-004-7-R6-Bagian 6.1	Setiap Entitas yang Bertanggung Jawab harus menerapkan satu atau lebih program manajemen akses terdokumentasi untuk mengotorisasi, memverifikasi, dan mencabut akses yang disediakan ke BCSI yang berkaitan dengan “Sistem yang Berlaku” yang diidentifikasi dalam CIP-004-7 Tabel R6 — Manajemen Akses untuk Informasi Sistem Cyber BES yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-004-7 Tabel R6 — Manajemen Akses untuk Informasi Sistem Cyber BES. Untuk dipertimbangkan akses ke BCSI dalam konteks persyaratan ini, seorang individu memiliki kemampuan untuk memperoleh	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
	dan menggunakan BCSI. Akses yang disediakan harus dianggap sebagai hasil dari tindakan spesifik yang diambil untuk menyediakan sarana bagi individu untuk mengakses BCSI (misalnya, dapat mencakup kunci fisik atau kartu akses, pengguna dan hak dan hak istimewa terkait, kunci enkripsi). Bagian 6.1: Sebelum penyediaa n, otorisasi (kecuali telah diizinkan sesuai dengan Bagian 4.1.) berdasark an kebutuhan , sebagaimana ditentukan oleh Entitas yang Bertanggung Jawab, kecuali untuk Keadaan Luar Biasa CIP: 6.1.1. Akses elektronik yang disediakan ke BCSI elektronik		

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-004-7-R6-Bagian 6.1	Setiap Entitas yang Bertanggung Jawab harus menerapkan satu atau lebih program manajemen akses terdokumentasi untuk mengotorisasi, memverifikasi, dan mencabut akses yang disediakan ke BCSI yang berkaitan dengan “Sistem yang Berlaku” yang diidentifikasi dalam CIP-004-7 Tabel R6 — Manajemen Akses untuk Informasi Sistem Cyber BES yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-004-7 Tabel R6 — Manajemen Akses untuk Informasi Sistem Cyber BES. Untuk dipertimbangkan akses ke BCSI dalam konteks persyaratan ini, seorang individu memiliki kemampuan untuk memperoleh	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
	dan menggunakan BCSI. Akses yang disediakan harus dianggap sebagai hasil dari tindakan spesifik yang diambil untuk menyediakan sarana bagi individu untuk mengakses BCSI (misalnya, dapat mencakup kunci fisik atau kartu akses, pengguna dan hak dan hak istimewa terkait, kunci enkripsi). Bagian 6.1: Sebelum penyediaa n, otorisasi (kecuali telah diizinkan sesuai dengan Bagian 4.1.) berdasark an kebutuhan , sebagaimana ditentukan oleh Entitas yang Bertanggung Jawab, kecuali untuk Keadaan Luar Biasa CIP: 6.1.1. Akses elektronik yang disediakan ke BCSI elektronik		

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-004-7-R6-Bagian 6.1	Setiap Entitas yang Bertanggung Jawab harus menerapkan satu atau lebih program manajemen akses terdokumentasi untuk mengotorisasi, memverifikasi, dan mencabut akses yang disediakan ke BCSI yang berkaitan dengan “Sistem yang Berlaku” yang diidentifikasi dalam CIP-004-7 Tabel R6 — Manajemen Akses untuk Informasi Sistem Cyber BES yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-004-7 Tabel R6 — Manajemen Akses untuk Informasi Sistem Cyber BES. Untuk dipertimbangkan akses ke BCSI dalam konteks persyaratan ini, seorang individu memiliki kemampuan untuk memperoleh	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
	dan menggunakan BCSI. Akses yang disediakan harus dianggap sebagai hasil dari tindakan spesifik yang diambil untuk menyediakan sarana bagi individu untuk mengakses BCSI (misalnya, dapat mencakup kunci fisik atau kartu akses, pengguna dan hak dan hak istimewa terkait, kunci enkripsi). Bagian 6.1: Sebelum penyediaa n, otorisasi (kecuali telah diizinkan sesuai dengan Bagian 4.1.) berdasark an kebutuhan , sebagaimana ditentukan oleh Entitas yang Bertanggung Jawab, kecuali untuk Keadaan Luar Biasa CIP: 6.1.1. Akses elektronik yang disediakan ke BCSI elektronik		

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-004-7-R6-Bagian 6.1	Setiap Entitas yang Bertanggung Jawab harus menerapkan satu atau lebih program manajemen akses terdokumentasi untuk mengotorisasi, memverifikasi, dan mencabut akses yang disediakan ke BCSI yang berkaitan dengan “Sistem yang Berlaku” yang diidentifikasi dalam CIP-004-7 Tabel R6 — Manajemen Akses untuk Informasi Sistem Cyber BES yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-004-7 Tabel R6 — Manajemen Akses untuk Informasi Sistem Cyber BES. Untuk dipertimbangkan akses ke BCSI dalam konteks persyaratan ini, seorang individu memiliki kemampuan untuk memperoleh	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
	dan menggunakan BCSI. Akses yang disediakan harus dianggap sebagai hasil dari tindakan spesifik yang diambil untuk menyediakan sarana bagi individu untuk mengakses BCSI (misalnya, dapat mencakup kunci fisik atau kartu akses, pengguna dan hak dan hak istimewa terkait, kunci enkripsi). Bagian 6.1: Sebelum penyediaa n, otorisasi (kecuali telah diizinkan sesuai dengan Bagian 4.1.) berdasark an kebutuhan , sebagaimana ditentukan oleh Entitas yang Bertanggung Jawab, kecuali untuk Keadaan Luar Biasa CIP: 6.1.1. Akses elektronik yang disediakan ke BCSI elektronik		

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-004-7-R6-Bagian 6.1	Setiap Entitas yang Bertanggung Jawab harus menerapkan satu atau lebih program manajemen akses terdokumentasi untuk mengotorisasi, memverifikasi, dan mencabut akses yang disediakan ke BCSI yang berkaitan dengan “Sistem yang Berlaku” yang diidentifikasi dalam CIP-004-7 Tabel R6 — Manajemen Akses untuk Informasi Sistem Cyber BES yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-004-7 Tabel R6 — Manajemen Akses untuk Informasi Sistem Cyber BES. Untuk dipertimbangkan akses ke BCSI dalam konteks persyaratan ini, seorang individu memiliki kemampuan untuk memperoleh	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
	dan menggunakan BCSI. Akses yang disediakan harus dianggap sebagai hasil dari tindakan spesifik yang diambil untuk menyediakan sarana bagi individu untuk mengakses BCSI (misalnya, dapat mencakup kunci fisik atau kartu akses, pengguna dan hak dan hak istimewa terkait, kunci enkripsi). Bagian 6.1: Sebelum penyediaa n, otorisasi (kecuali telah diizinkan sesuai dengan Bagian 4.1.) berdasark an kebutuhan , sebagaimana ditentukan oleh Entitas yang Bertanggung Jawab, kecuali untuk Keadaan Luar Biasa CIP: 6.1.1. Akses elektronik yang disediakan ke BCSI elektronik		

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-004-7-R6-Bagian 6.1	Setiap Entitas yang Bertanggung Jawab harus menerapkan satu atau lebih program manajemen akses terdokumentasi untuk mengotorisasi, memverifikasi, dan mencabut akses yang disediakan ke BCSI yang berkaitan dengan “Sistem yang Berlaku” yang diidentifikasi dalam CIP-004-7 Tabel R6 — Manajemen Akses untuk Informasi Sistem Cyber BES yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-004-7 Tabel R6 — Manajemen Akses untuk Informasi Sistem Cyber BES. Untuk dipertimbangkan akses ke BCSI dalam konteks persyaratan ini, seorang individu memiliki kemampuan untuk memperoleh	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
	dan menggunakan BCSI. Akses yang disediakan harus dianggap sebagai hasil dari tindakan spesifik yang diambil untuk menyediakan sarana bagi individu untuk mengakses BCSI (misalnya, dapat mencakup kunci fisik atau kartu akses, pengguna dan hak dan hak istimewa terkait, kunci enkripsi). Bagian 6.1: Sebelum penyediaa n, otorisasi (kecuali telah diizinkan sesuai dengan Bagian 4.1.) berdasark an kebutuhan , sebagaimana ditentukan oleh Entitas yang Bertanggung Jawab, kecuali untuk Keadaan Luar Biasa CIP: 6.1.1. Akses elektronik yang disediakan ke BCSI elektronik		

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	iam-user-unused-cr edentials-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharus kan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	lambda-function-pu blic-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotens i menyebabkan degradasi ketersedi aan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	s3- account-level-publ ic-access -blok-per iodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	sagemaker-notebook -no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	acm-certificate-ex piration-check	Pastikan integritas jaringan dilindungi dengan memastika n sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExp iration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	alb-http-drop-invalid-header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	api-gw-cache-enabl ed-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrai l jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	cmk-backing-key-ro tation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	dynamodb-table-enc rypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindung i data tersebut. Secara default, tabel DynamoDB dienkrips i dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	ecr-private-image-scanning-diaktifkan	Pemindaian gambar Amazon Elastic Container Repositor y (ECR) membantu mengidentifikasi kerentanan perangkat lunak dalam gambar kontainer Anda. Mengaktifkan pemindaian gambar pada repositori ECR menambahk an lapisan verifikasi untuk integritas dan keamanan gambar yang disimpan.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	ecr-private-tag-im mutability-diaktifkan	Aktifkan Kekekalan Tag Elastic Container Repository (ECR) untuk mencegah tag gambar pada gambar ECR Anda ditimpa. Sebelumny a, tag dapat ditimpa yang membutuhkan metodologi manual untuk mengidentifikasi gambar secara unik.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	ecs-containers-rea donly-access	Mengaktifkan akses baca saja ke wadah Amazon Elastic Container Service (ECS) dapat membantu mematuhi prinsip hak istimewa yang paling rendah. Opsi ini dapat mengurangi vektor serangan karena sistem file instance container tidak dapat dimodifikasi kecuali jika memiliki izin baca-tulis eksplisit.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	elasticsearch-encr ypted-at-rest	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk domain OpenSearc h Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-n ode enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkrip si memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	kinesis-stream-enc rypted	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	kms-cmk-not-schedu led-untuk-penghapu san	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	opensearch-audit-l ogging-enabled	Pastikan pencatata n audit diaktifkan di domain OpenSearc h Layanan Amazon Anda. Pencatatan audit memungkin kan Anda melacak aktivitas pengguna di OpenSearc h domain Anda, termasuk keberhasi lan dan kegagalan otentikasi, permintaa n, perubahan indeks OpenSearch, dan kueri penelusuran yang masuk.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	opensearch-encrypt ed-at-rest	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk domain OpenSearc h Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	opensearch-https-r equired	Karena data sensitif dapat ada dan membantu melindung i data dalam perjalana n, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearc h Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara Amazon OpenSearch dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	opensearch-node-to -node-pemeriksaan enkripsi-	Pastikan node-to-n ode enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkrip si memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	rds-snapshot-encry pted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	redshift-audit-logging-enabled	Untuk menangkap informasi tentang koneksi dan aktivitas pengguna di klaster Amazon Redshift, pastikan pencatatan audit diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	redshift-cluster-c onfiguration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastika n bahwa konfigura si yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberika n informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapka n untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	s3- bucket-ssl-request s-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	s3- default-encryption -kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	s3- event-notification s-enabled	Pemberitahuan peristiwa Amazon S3 dapat memberi tahu personel terkait tentang modifikasi yang tidak disengaja atau disengaja pada objek bucket Anda. Contoh peringatan meliputi: objek baru adalah pembuatan, penghapusan objek, restorasi objek, objek yang hilang dan direplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	s3- lifecycle-policy-c heck	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihk an objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	sagemaker-endpoint -configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	sagemaker-notebook -instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	rds-cluster-default-admin-periksa	Karena nama pengguna default adalah pengetahu an publik, mengubah nama pengguna default dapat membantu mengurangi permukaan serangan untuk kluster database Amazon Relational Database Service (Amazon RDS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	rds-instance-default-admin-periksa	Karena nama pengguna default adalah pengetahu an publik, mengubah nama pengguna default dapat membantu mengurangi permukaan serangan untuk instans database Amazon Relational Database Service (Amazon RDS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	redshift-default-a dmin-check	Karena nama pengguna default adalah pengetahu an publik, mengubah nama pengguna default dapat membantu mengurangi permukaan serangan untuk klaster Amazon Redshift Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CIP-011-3-R1-Bagian 1.2	Setiap Entitas yang Bertanggung Jawab harus melaksana kan satu atau lebih program perlindungan informasi terdokume ntasi yang secara kolektif mencakup masing-masing bagian persyaratan yang berlaku dalam CIP-011-3 Tabel R1 — Perlindungan Informasi. Bagian 1.2: Metode untuk melindungi dan menangani BCSI dengan aman untuk mengurangi risiko membahayakan kerahasiaan.	s3- bucket-acl-prohibi ted	Aturan ini memeriksa untuk melihat apakah Daftar Kontrol Akses (ACLs) digunakan untuk kontrol akses di Bucket Amazon S3. ACLs adalah mekanisme kontrol akses lama untuk bucket Amazon S3 yang AWS mendahulu i Identity and Access Management (IAM). Sebagai gantinya ACLs, ini adalah praktik terbaik untuk menggunakan kebijakan IAM atau kebijakan bucket S3 untuk mengelola akses ke bucket S3 Anda dengan lebih mudah.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk NERC CIP BCSI.

Praktik Terbaik Operasional untuk Prinsip Keamanan Cloud NCSC

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk

membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara Prinsip Keamanan Cloud Pusat Keamanan Cyber Nasional Inggris (NCSC) dan aturan AWS Config yang dikelola. Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau beberapa kontrol Prinsip Keamanan Cloud NCSC Inggris. Kontrol Prinsip Keamanan Cloud NCSC Inggris dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

Contoh template paket kesesuaian ini berisi pemetaan ke kontrol dalam Prinsip Keamanan Cloud NCSC Inggris (Pusat Keamanan Cyber Nasional | Panduan keamanan cloud), dengan informasi sektor publik yang dilisensikan di bawah Lisensi Pemerintah Terbuka v3.0. Lisensi Pemerintah Terbuka harus dapat diakses di sini: Lisensi Pemerintah Terbuka untuk informasi sektor publik.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1. Data dalam perlindungan transit	Jaringan transit data pengguna harus dilindungi secara memadai terhadap gangguan dan penyadapan.	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
1. Data dalam perlindungan transit	Jaringan transit data pengguna harus dilindungi secara memadai terhadap	acm-certificate-ex piration-check	Pastikan integritas jaringan dilindungi dengan memastika n sertifikat X509

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	gangguan dan penyadapan.		dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExp iration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
1. Data dalam perlindungan transit	Jaringan transit data pengguna harus dilindungi secara memadai terhadap gangguan dan penyadapan.	alb-http-to-https-pemeriksaan-pengalihan	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1. Data dalam perlindungan transit	Jaringan transit data pengguna harus dilindungi secara memadai terhadap gangguan dan penyadapan.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
1. Data dalam perlindungan transit	Jaringan transit data pengguna harus dilindungi secara memadai terhadap gangguan dan penyadapan.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-n ode enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkrip si memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1. Data dalam perlindungan transit	Jaringan transit data pengguna harus dilindungi secara memadai terhadap gangguan dan penyadapan.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
1. Data dalam perlindungan transit	Jaringan transit data pengguna harus dilindungi secara memadai terhadap gangguan dan penyadapan.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1. Data dalam perlindungan transit	Jaringan transit data pengguna harus dilindungi secara memadai terhadap gangguan dan penyadapan.	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
1. Data dalam perlindungan transit	Jaringan transit data pengguna harus dilindungi secara memadai terhadap gangguan dan penyadapan.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1. Data dalam perlindungan transit	Jaringan transit data pengguna harus dilindungi secara memadai terhadap gangguan dan penyadapan.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
1. Data dalam perlindungan transit	Jaringan transit data pengguna harus dilindungi secara memadai terhadap gangguan dan penyadapan.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	codebuild-project-artifact-encryption	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk AWS CodeBuild artefak Anda.
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	kinesis-stream-encrypted	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDbEncrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	s3- default-encryption -kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2. Perlindungan dan ketahanan aset	Data Anda (dan aset yang menyimpan atau memprosesnya) harus dilindungi secara memadai.	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	api-gw-execution-l ogging-diaktifkan	Pencatatan API Gateway menampilk an tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteks i aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	cw-loggroup-retent ion-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonst ruksi dan mengident ifikasi peristiwa yang berpotensi berbahaya.
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifka n untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventari s platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	ec2- -periksa managedinstance-pa tch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberika n visibilitas terperinc i ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpan an Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitorin g mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	redshift-cluster-m aintenancesettings-check	Aturan ini memastika n bahwa klaster Amazon Redshift memiliki pengatura n yang diinginka n untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemelihar aan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrad e. Bawaannya adalah benar. Ini juga memungkin kan Anda secara opsional mengatur preferredMaintenan ceWindow (defaultn ya adalah sat: 16:00 -sat: 16:30), dan automatedSnapshotR etention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediak an metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinc i untuk permintaa n yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5. Keamanan operasional	Layanan harus dioperasikan dan dikelola dengan cara untuk menghamba t, mendeteksi atau mencegah serangan.	wafv2-logging-diak tifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatata n AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7. Pengembangan yang aman	Layanan cloud harus dirancang, dikembang kan, dan digunakan dengan cara yang meminimalkan dan mengurangi ancaman terhadap keamanan mereka.	codebuild-project-environment-privil eged-periksa	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan lingkungan CodeBuild proyek Amazon Anda tidak mengaktif kan mode istimewa. Pengaturan ini harus dinonaktifkan untuk mencegah akses yang tidak diinginkan ke Docker APIs serta perangkat keras yang mendasarinya.
7. Pengembangan yang aman	Layanan cloud harus dirancang, dikembang kan, dan digunakan dengan cara yang meminimalkan dan mengurangi ancaman terhadap keamanan mereka.	codebuild-project-envvar-awscred-per iksa	Pastikan kredensya l otentikasi AWS_ACCES S_KEY_ID dan AWS_SECRE T_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild . Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabk an paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7. Pengembangan yang aman	Layanan cloud harus dirancang, dikembang kan, dan digunakan dengan cara yang meminimalkan dan mengurangi ancaman terhadap keamanan mereka.	codebuild-project-source-repo-url-pe riksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredensyal masuk dalam lingkungan proyek Codebuild . AWS Gunakan OAuth alih-alih token akses pribadi atau kredensyal masuk untuk memberika n otorisasi untuk mengakses GitHub atau repositori Bitbucket.
9. Manajemen pengguna yang aman	Penyedia harus menyediakan alat untuk mengelola penggunaan layanan mereka dengan aman.	account-part-of-or ganizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastika n bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
9. Manajemen pengguna yang aman	Penyedia harus menyediakan alat untuk mengelola penggunaan layanan mereka dengan aman.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
9. Manajemen pengguna yang aman	Penyedia harus menyediakan alat untuk mengelola penggunaan layanan mereka dengan aman.	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
9. Manajemen pengguna yang aman	Penyedia harus menyediakan alat untuk mengelola penggunaan layanan mereka dengan aman.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
9. Manajemen pengguna yang aman	Penyedia harus menyediakan alat untuk mengelola penggunaan layanan mereka dengan aman.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredensi masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
9. Manajemen pengguna yang aman	Penyedia harus menyediakan alat untuk mengelola penggunaan layanan mereka dengan aman.	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
9. Manajemen pengguna yang aman	Penyedia harus menyediakan alat untuk mengelola penggunaan layanan mereka dengan aman.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
9. Manajemen pengguna yang aman	Penyedia harus menyediakan alat untuk mengelola penggunaan layanan mereka dengan aman.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
9. Manajemen pengguna yang aman	Penyedia harus menyediakan alat untuk mengelola penggunaan layanan mereka dengan aman.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
9. Manajemen pengguna yang aman	Penyedia harus menyediakan alat untuk mengelola penggunaan layanan mereka dengan aman.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
9. Manajemen pengguna yang aman	Penyedia harus menyediakan alat untuk mengelola penggunaan layanan mereka dengan aman.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
9. Manajemen pengguna yang aman	Penyedia harus menyediakan alat untuk mengelola penggunaan layanan mereka dengan aman.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsageUsia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10. Identitas dan otentikasi	Akses ke antarmuka layanan harus dibatasi untuk individu yang diautentikasi dan diotorisasi.	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10. Identitas dan otentikasi	Akses ke antarmuka layanan harus dibatasi untuk individu yang diautentikasi dan diotorisasi.	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10. Identitas dan otentikasi	Akses ke antarmuka layanan harus dibatasi untuk individu yang diautentikasi dan diotorisasi.	rds-instance-iam-authentication-diaktifkan	Pastikan autentikasi AWS Identity and Access Management (IAM) diaktifkan pada instans Amazon Relational Database Service (Amazon RDS) untuk mengontrol akses ke sistem dan aset. Ini memberlakukan lalu lintas jaringan ke dan dari database yang akan dienkripsi menggunakan Secure Sockets Layer (SSL). Anda tidak diharuskan untuk menyimpan kredensi pengguna dalam database, karena otentikasi dikelola secara eksternal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10. Identitas dan otentikasi	Akses ke antarmuka layanan harus dibatasi untuk individu yang diautentikasi dan diotorisasi.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10. Identitas dan otentikasi	Akses ke antarmuka layanan harus dibatasi untuk individu yang diautentikasi dan diotorisasi.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10. Identitas dan otentikasi	Akses ke antarmuka layanan harus dibatasi untuk individu yang diautentikasi dan diotorisasi.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10. Identitas dan otentikasi	Akses ke antarmuka layanan harus dibatasi untuk individu yang diautentikasi dan diotorisasi.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10. Identitas dan otentikasi	Akses ke antarmuka layanan harus dibatasi untuk individu yang diautentikasi dan diotorisasi.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredensi masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10. Identitas dan otentikasi	Akses ke antarmuka layanan harus dibatasi untuk individu yang diautentikasi dan diotorisasi.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10. Identitas dan otentikasi	Akses ke antarmuka layanan harus dibatasi untuk individu yang diautentikasi dan diotorisasi.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11. Perlindungan antarmuka eksternal	Semua antarmuka eksternal atau kurang tepercaya ke layanan harus diidentifikasi dan dipertahankan.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11. Perlindungan antarmuka eksternal	Semua antarmuka eksternal atau kurang tepercaya ke layanan harus diidentifikasi dan dipertahankan.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11. Perlindungan antarmuka eksternal	Semua antarmuka eksternal atau kurang tepercaya ke layanan harus diidentifikasi dan dipertahankan.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11. Perlindungan antarmuka eksternal	Semua antarmuka eksternal atau kurang tepercaya ke layanan harus diidentifikasi dan dipertahankan.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11. Perlindungan antarmuka eksternal	Semua antarmuka eksternal atau kurang tepercaya ke layanan harus diidentifikasi dan dipertahankan.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11. Perlindungan antarmuka eksternal	Semua antarmuka eksternal atau kurang tepercaya ke layanan harus diidentifikasi dan dipertahankan.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
11. Perlindungan antarmuka eksternal	Semua antarmuka eksternal atau kurang tepercaya ke layanan harus diidentifikasi dan dipertahankan.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11. Perlindungan antarmuka eksternal	Semua antarmuka eksternal atau kurang tepercaya ke layanan harus diidentifikasi dan dipertahankan.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
11. Perlindungan antarmuka eksternal	Semua antarmuka eksternal atau kurang tepercaya ke layanan harus diidentifikasi dan dipertahankan.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11. Perlindungan antarmuka eksternal	Semua antarmuka eksternal atau kurang tepercaya ke layanan harus diidentifikasi dan dipertahankan.	ecs-container-insights-enabled	Pemantauan merupakan bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja Amazon Elastic Container Service (ECS) dan AWS solusi Anda. Wawasan Kontainer juga akan menyediakan informasi diagnostik, seperti kegagalan mengulang kembali kontainer, untuk membantu Anda melakukan isolasi atas masalah dan mengatasi masalah itu dengan cepat.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11. Perlindungan antarmuka eksternal	Semua antarmuka eksternal atau kurang tepercaya ke layanan harus diidentifikasi dan dipertahankan.	ecs-containers-non privileged	Untuk membantu menerapkan prinsip hak istimewa paling rendah, definisi tugas Amazon Elastic Container Service (Amazon ECS) seharusnya tidak mengaktifkan hak istimewa yang ditinggikan. Ketika parameter ini benar, wadah diberikan hak istimewa yang ditinggikan pada instance wadah host (mirip dengan pengguna root).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11. Perlindungan antarmuka eksternal	Semua antarmuka eksternal atau kurang tepercaya ke layanan harus diidentifikasi dan dipertahankan.	ecs-containers-readonly-access	Mengaktifkan akses baca saja ke kontainer Amazon Elastic Container Service (ECS) dapat membantu mematuhi prinsip hak istimewa yang paling rendah. Opsi ini dapat mengurangi vektor serangan karena sistem file instance container tidak dapat dimodifikasi kecuali jika memiliki izin baca-tulis eksplisit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11. Perlindungan antarmuka eksternal	Semua antarmuka eksternal atau kurang tepercaya ke layanan harus diidentifikasi dan dipertahankan.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
11. Perlindungan antarmuka eksternal	Semua antarmuka eksternal atau kurang tepercaya ke layanan harus diidentifikasi dan dipertahankan.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11. Perlindungan antarmuka eksternal	Semua antarmuka eksternal atau kurang tepercaya ke layanan harus diidentifikasi dan dipertahankan.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11. Perlindungan antarmuka eksternal	Semua antarmuka eksternal atau kurang tepercaya ke layanan harus diidentifikasi dan dipertahankan.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
11. Perlindungan antarmuka eksternal	Semua antarmuka eksternal atau kurang tepercaya ke layanan harus diidentifikasi dan dipertahankan.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11. Perlindungan antarmuka eksternal	Semua antarmuka eksternal atau kurang tepercaya ke layanan harus diidentifikasi dan dipertahankan.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11. Perlindungan antarmuka eksternal	Semua antarmuka eksternal atau kurang tepercaya ke layanan harus diidentifikasi dan dipertahankan.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11. Perlindungan antarmuka eksternal	Semua antarmuka eksternal atau kurang tepercaya ke layanan harus diidentifikasi dan dipertahankan.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
11. Perlindungan antarmuka eksternal	Semua antarmuka eksternal atau kurang tepercaya ke layanan harus diidentifikasi dan dipertahankan.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11. Perlindungan antarmuka eksternal	Semua antarmuka eksternal atau kurang tepercaya ke layanan harus diidentifikasi dan dipertahankan.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
11. Perlindungan antarmuka eksternal	Semua antarmuka eksternal atau kurang tepercaya ke layanan harus diidentifikasi dan dipertahankan.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11. Perlindungan antarmuka eksternal	Semua antarmuka eksternal atau kurang tepercaya ke layanan harus diidentifikasi dan dipertahankan.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
11. Perlindungan antarmuka eksternal	Semua antarmuka eksternal atau kurang tepercaya ke layanan harus diidentifikasi dan dipertahankan.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11. Perlindungan antarmuka eksternal	Semua antarmuka eksternal atau kurang tepercaya ke layanan harus diidentifikasi dan dipertahankan.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11. Perlindungan antarmuka eksternal	Semua antarmuka eksternal atau kurang tepercaya ke layanan harus diidentifikasi dan dipertahankan.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11. Perlindungan antarmuka eksternal	Semua antarmuka eksternal atau kurang tepercaya ke layanan harus diidentifikasi dan dipertahankan.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12. Administrasi layanan yang aman	Penyedia cloud harus mengenali nilai tinggi dari sistem administr asi.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
13. Informasi audit untuk pengguna	Penyedia harus menyediakan log yang diperlukan untuk memantau akses ke layanan Anda, dan data yang disimpan di dalamnya.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
13. Informasi audit untuk pengguna	Penyedia harus menyediakan log yang diperlukan untuk memantau akses ke layanan Anda, dan data yang disimpan di dalamnya.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
13. Informasi audit untuk pengguna	Penyedia harus menyediakan log yang diperlukan untuk memantau akses ke layanan Anda, dan data yang disimpan di dalamnya.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
13. Informasi audit untuk pengguna	Penyedia harus menyediakan log yang diperlukan untuk memantau akses ke layanan Anda, dan data yang disimpan di dalamnya.	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomen dasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaa n enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Prinsip Keamanan Cloud NCSC.

Praktik Terbaik Operasional untuk Kerangka Penilaian Cyber NCSC

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara kontrol Cyber Security Center (NCSC) Cyber Assessment Framework (CAF) Inggris dan aturan Config yang dikelola AWS . Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau beberapa kontrol CAF NCSC UK. Kontrol CAF NCSC Inggris dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

Templat paket kesesuaian sampel ini berisi pemetaan ke kontrol dalam UK NCSC CAF (Pusat Keamanan Cyber Nasional | panduan CAF NCSC), dengan informasi sektor publik tersebut dilisensikan di bawah Lisensi Pemerintah Terbuka v3.0. Lisensi Pemerintah Terbuka harus dapat diakses di sini: Lisensi Pemerintah Terbuka untuk informasi sektor publik.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.a Manajemen Aset	Segala sesuatu yang diperlukan untuk memberikan, memelihara, atau mendukung jaringan dan sistem informasi yang diperlukan untuk pengoperasian fungsi-fungsi penting ditentukan dan dipahami. Ini termasuk data, orang dan sistem, serta infrastruktur pendukung (seperti daya atau pendinginan).	vpc-network-acl-unused-periksa	Aturan ini memastikan bahwa daftar kontrol akses jaringan Amazon Virtual Private Cloud (VPC) sedang digunakan. Pemantauan untuk daftar kontrol akses jaringan yang tidak digunakan dapat membantu inventaris dan pengelolaan lingkungan Anda yang akurat.
A3.a Manajemen Aset	Segala sesuatu yang diperlukan untuk memberikan, memelihara, atau mendukung jaringan dan sistem informasi yang diperlukan untuk pengoperasian fungsi-fungsi penting ditentukan dan dipahami. Ini termasuk data,	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	orang dan sistem, serta infrastruktur pendukung apa pun (seperti daya atau pendinginan).		Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.
A3.a Manajemen Aset	Segala sesuatu yang diperlukan untuk memberikan, memelihara, atau mendukung jaringan dan sistem informasi yang diperlukan untuk pengopera sian fungsi-fungsi penting ditentuka n dan dipahami. Ini termasuk data, orang dan sistem, serta infrastruktur pendukung apa pun (seperti daya atau pendinginan).	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.a Manajemen Aset	Segala sesuatu yang diperlukan untuk memberikan, memelihara, atau mendukung jaringan dan sistem informasi yang diperlukan untuk pengoperasian fungsi-fungsi penting ditentukan dan dipahami. Ini termasuk data, orang dan sistem, serta infrastruktur pendukung apa pun (seperti daya atau pendinginan).	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.a Manajemen Aset	Segala sesuatu yang diperlukan untuk memberikan, memelihara, atau mendukung jaringan dan sistem informasi yang diperlukan untuk pengoperasian fungsi-fungsi penting ditentukan dan dipahami. Ini termasuk data, orang dan sistem, serta infrastruktur pendukung apa pun (seperti daya atau pendinginan).	terlampir eip	Aturan ini memastikan Elastic yang IPs dialokasikan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan. Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B2.a Verifikasi Identitas, Otentikasi dan Otorisasi	Anda dengan kuat memverifikasi, mengautentikasi, dan mengotorisasi akses ke jaringan dan sistem informasi yang mendukung fungsi penting Anda.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B2.a Verifikasi Identitas, Otentikasi dan Otorisasi	Anda dengan kuat memverifikasi, mengautentikasi, dan mengotorisasi akses ke jaringan dan sistem informasi yang mendukung fungsi penting Anda.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B2.a Verifikasi Identitas, Otentikasi dan Otorisasi	Anda dengan kuat memverifikasi, mengautentikasi, dan mengotorisasi akses ke jaringan dan sistem informasi yang mendukung fungsi penting Anda.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B2.a Verifikasi Identitas, Otentikasi dan Otorisasi	Anda dengan kuat memverifikasi, mengautentikasi, dan mengotorisasi akses ke jaringan dan sistem informasi yang mendukung fungsi penting Anda.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B2.a Verifikasi Identitas, Otentikasi dan Otorisasi	Anda dengan kuat memverifikasi, mengautentikasi, dan mengotorisasi akses ke jaringan dan sistem informasi yang mendukung fungsi penting Anda.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B2.a Verifikasi Identitas, Otentikasi dan Otorisasi	Anda dengan kuat memverifikasi, mengautentikasi, dan mengotorisasi akses ke jaringan dan sistem informasi yang mendukung fungsi penting Anda.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsageUsia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B2.a Verifikasi Identitas, Otentikasi dan Otorisasi	Anda dengan kuat memverifikasi, mengautentikasi, dan mengotorisasi akses ke jaringan dan sistem informasi yang mendukung fungsi penting Anda.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B2.a Verifikasi Identitas, Otentikasi dan Otorisasi	Anda dengan kuat memverifikasi, mengautentikasi, dan mengotorisasi akses ke jaringan dan sistem informasi yang mendukung fungsi penting Anda.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B2.a Verifikasi Identitas, Otentikasi dan Otorisasi	Anda dengan kuat memverifikasi, mengautentikasi, dan mengotorisasi akses ke jaringan dan sistem informasi yang mendukung fungsi penting Anda.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B2.a Verifikasi Identitas, Otentikasi dan Otorisasi	Anda dengan kuat memverifikasi, mengautentikasi, dan mengotorisasi akses ke jaringan dan sistem informasi yang mendukung fungsi penting Anda.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B2.a Verifikasi Identitas, Otentikasi dan Otorisasi	Anda dengan kuat memverifikasi, mengautentikasi, dan mengotorisasi akses ke jaringan dan sistem informasi yang mendukung fungsi penting Anda.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B2.a Verifikasi Identitas, Otentikasi dan Otorisasi	Anda dengan kuat memverifikasi, mengautentikasi, dan mengotorisasi akses ke jaringan dan sistem informasi yang mendukung fungsi penting Anda.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B2.a Verifikasi Identitas, Otentikasi dan Otorisasi	Anda dengan kuat memverifikasi, mengautentikasi, dan mengotorisasi akses ke jaringan dan sistem informasi yang mendukung fungsi penting Anda.	opensearch-access-control-enabled	Pastikan kontrol akses berbutir halus diaktifkan di domain Layanan Amazon OpenSearch Anda. Kontrol akses berbutir halus menyediakan mekanisme otorisasi yang disempurnakan untuk mencapai akses yang paling tidak memiliki hak istimewa ke domain Layanan Amazon. OpenSearch Ini memungkinkan kontrol akses berbasis peran ke domain, serta indeks, dokumen, dan keamanan tingkat lapangan, dukungan untuk dasbor OpenSearch Layanan multi-tenancy, dan otentikasi dasar HTTP untuk Layanan dan Kibana. OpenSearch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B2.a Verifikasi Identitas, Otentikasi dan Otorisasi	Anda dengan kuat memverifikasi, mengautentikasi, dan mengotorisasi akses ke jaringan dan sistem informasi yang mendukung fungsi penting Anda.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Manajemen Perangkat B2.b	Anda sepenuhnya tahu dan memiliki kepercayaan pada perangkat yang digunakan untuk mengakses jaringan, sistem informasi, dan data Anda yang mendukung fungsi penting Anda.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Manajemen Perangkat B2.b	Anda sepenuhnya tahu dan memiliki kepercayaan pada perangkat yang digunakan untuk mengakses jaringan, sistem informasi, dan data Anda yang mendukung fungsi penting Anda.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Manajemen Pengguna Istimewa B2.c	Anda dengan cermat mengelola akses pengguna istimewa ke jaringan dan sistem informasi yang mendukung fungsi penting.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsageUsia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Manajemen Pengguna Istimewa B2.c	Anda dengan cermat mengelola akses pengguna istimewa ke jaringan dan sistem informasi yang mendukung fungsi penting.	codebuild-project-environment-privileged-periksa	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan lingkungan CodeBuild proyek Amazon Anda tidak mengaktifkan mode istimewa. Pengaturan ini harus dinonaktifkan untuk mencegah akses yang tidak diinginkan ke Docker APIs serta perangkat keras yang mendasarinya.
Manajemen Pengguna Istimewa B2.c	Anda dengan cermat mengelola akses pengguna istimewa ke jaringan dan sistem informasi yang mendukung fungsi penting.	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Manajemen Pengguna Istimewa B2.c	Anda dengan cermat mengelola akses pengguna istimewa ke jaringan dan sistem informasi yang mendukung fungsi penting.	ecs-containers-non privileged	Untuk membantu menerapkan prinsip hak istimewa paling rendah, definisi tugas Amazon Elastic Container Service (Amazon ECS) seharusnya tidak mengaktifkan hak istimewa yang ditinggikan. Ketika parameter ini benar, wadah diberikan hak istimewa yang ditinggikan pada instance wadah host (mirip dengan pengguna root).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Manajemen Pengguna Istimewa B2.c	Anda dengan cermat mengelola akses pengguna istimewa ke jaringan dan sistem informasi yang mendukung fungsi penting.	ecs-containers-readonly-access	Mengaktifkan akses baca saja ke kontainer Amazon Elastic Container Service (ECS) dapat membantu mematuhi prinsip hak istimewa yang paling rendah. Opsi ini dapat mengurangi vektor serangan karena sistem file instance container tidak dapat dimodifikasi kecuali jika memiliki izin baca-tulis eksplisit.
Manajemen Pengguna Istimewa B2.c	Anda dengan cermat mengelola akses pengguna istimewa ke jaringan dan sistem informasi yang mendukung fungsi penting.	ecs-task-definition-nonroot-pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan bahwa pengguna non-root ditunjuk untuk mengakses definisi tugas Amazon Elastic Container Service (Amazon ECS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Manajemen Pengguna Istimewa B2.c	Anda dengan cermat mengelola akses pengguna istimewa ke jaringan dan sistem informasi yang mendukung fungsi penting.	efs-access-point-enforce-identitas pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan penegakan pengguna diaktifkan untuk Amazon Elastic File System (Amazon EFS) Anda. Saat diaktifkan, Amazon EFS mengganti kan pengguna dan grup klien NFS IDs dengan identitas yang dikonfigurasi pada titik akses untuk semua operasi sistem file dan hanya memberika n akses ke identitas pengguna yang diberlakukan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Manajemen Pengguna Istimewa B2.c	Anda dengan cermat mengelola akses pengguna istimewa ke jaringan dan sistem informasi yang mendukung fungsi penting.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Manajemen Pengguna Istimewa B2.c	Anda dengan cermat mengelola akses pengguna istimewa ke jaringan dan sistem informasi yang mendukung fungsi penting.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
Manajemen Pengguna Istimewa B2.c	Anda dengan cermat mengelola akses pengguna istimewa ke jaringan dan sistem informasi yang mendukung fungsi penting.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Manajemen Pengguna Istimewa B2.c	Anda dengan cermat mengelola akses pengguna istimewa ke jaringan dan sistem informasi yang mendukung fungsi penting.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Manajemen Pengguna Istimewa B2.c	Anda dengan cermat mengelola akses pengguna istimewa ke jaringan dan sistem informasi yang mendukung fungsi penting.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
Manajemen Pengguna Istimewa B2.c	Anda dengan cermat mengelola akses pengguna istimewa ke jaringan dan sistem informasi yang mendukung fungsi penting.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Manajemen Pengguna Istimewa B2.c	Anda dengan cermat mengelola akses pengguna istimewa ke jaringan dan sistem informasi yang mendukung fungsi penting.	secretsmanager-secret-unused	Jika kredensi yang tidak digunakan ada di AWS Secrets Manager, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini memungkinkan Anda untuk menetapkan nilai ke unusedFor Days (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Manajemen Pengguna Istimewa B2.c	Anda dengan cermat mengelola akses pengguna istimewa ke jaringan dan sistem informasi yang mendukung fungsi penting.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Manajemen Pengguna Istimewa B2.c	Anda dengan cermat mengelola akses pengguna istimewa ke jaringan dan sistem informasi yang mendukung fungsi penting.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Manajemen Pengguna Istimewa B2.c	Anda dengan cermat mengelola akses pengguna istimewa ke jaringan dan sistem informasi yang mendukung fungsi penting.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Manajemen Pengguna Istimewa B2.c	Anda dengan cermat mengelola akses pengguna istimewa ke jaringan dan sistem informasi yang mendukung fungsi penting.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Manajemen Pengguna Istimewa B2.c	Anda dengan cermat mengelola akses pengguna istimewa ke jaringan dan sistem informasi yang mendukung fungsi penting.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Manajemen Pengguna Istimewa B2.c	Anda dengan cermat mengelola akses pengguna istimewa ke jaringan dan sistem informasi yang mendukung fungsi penting.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Manajemen Pengguna Istimewa B2.c	Anda dengan cermat mengelola akses pengguna istimewa ke jaringan dan sistem informasi yang mendukung fungsi penting.	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Manajemen Pengguna Istimewa B2.c	Anda dengan cermat mengelola akses pengguna istimewa ke jaringan dan sistem informasi yang mendukung fungsi penting.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B2.d Identity and Access Management (iDam)	Anda menjamin manajemen dan pemeliharaan identitas dan kontrol akses yang baik untuk jaringan dan sistem informasi Anda yang mendukung fungsi penting.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B2.d Identity and Access Management (iDam)	Anda menjamin manajemen dan pemeliharaan identitas dan kontrol akses yang baik untuk jaringan dan sistem informasi Anda yang mendukung fungsi penting.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B2.d Identity and Access Management (iDam)	Anda menjamin manajemen dan pemeliharaan identitas dan kontrol akses yang baik untuk jaringan dan sistem informasi Anda yang mendukung fungsi penting.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B2.d Identity and Access Management (iDam)	Anda menjamin manajemen dan pemeliharaan identitas dan kontrol akses yang baik untuk jaringan dan sistem informasi Anda yang mendukung fungsi penting.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B2.d Identity and Access Management (iDam)	Anda menjamin manajemen dan pemeliharaan identitas dan kontrol akses yang baik untuk jaringan dan sistem informasi Anda yang mendukung fungsi penting.	iam-user-unused-credentials-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharus kan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B2.d Identity and Access Management (iDam)	Anda menjamin manajemen dan pemeliharaan identitas dan kontrol akses yang baik untuk jaringan dan sistem informasi Anda yang mendukung fungsi penting.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B2.d Identity and Access Management (iDam)	Anda menjamin manajemen dan pemeliharaan identitas dan kontrol akses yang baik untuk jaringan dan sistem informasi Anda yang mendukung fungsi penting.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B2.d Identity and Access Management (iDam)	Anda menjamin manajemen dan pemeliharaan identitas dan kontrol akses yang baik untuk jaringan dan sistem informasi Anda yang mendukung fungsi penting.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B2.d Identity and Access Management (iDam)	Anda menjamin manajemen dan pemeliharaan identitas dan kontrol akses yang baik untuk jaringan dan sistem informasi Anda yang mendukung fungsi penting.	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B2.d Identity and Access Management (iDam)	Anda menjamin manajemen dan pemeliharaan identitas dan kontrol akses yang baik untuk jaringan dan sistem informasi Anda yang mendukung fungsi penting.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B2.d Identitas dan Manajemen Akses (iDam)	Anda menjamin manajemen dan pemeliharaan identitas dan kontrol akses yang baik untuk jaringan dan sistem informasi Anda yang mendukung fungsi penting.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B2.d Identity and Access Management (iDam)	Anda menjamin manajemen dan pemeliharaan identitas dan kontrol akses yang baik untuk jaringan dan sistem informasi Anda yang mendukung fungsi penting.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B2.d Identity and Access Management (iDam)	Anda menjamin manajemen dan pemeliharaan identitas dan kontrol akses yang baik untuk jaringan dan sistem informasi Anda yang mendukung fungsi penting.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B3.a Memahami Data	Anda memiliki pemahaman yang baik tentang data yang penting untuk pengoperasian fungsi penting, di mana ia disimpan, di mana ia bergerak dan bagaimana tidak tersedianya atau akses yang tidak sah, modifikasi atau penghapusan akan berdampak buruk pada fungsi penting. Ini juga berlaku untuk pihak ketiga yang menyimpan atau mengakses data yang penting untuk pengoperasian fungsi-fungsi penting.	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data B3.b dalam Transit	Anda telah melindungi transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
Data B3.b dalam Transit	Anda telah melindungi transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	alb-http-drop-invalid-Header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data B3.b dalam Transit	Anda telah melindung i transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Data B3.b dalam Transit	Anda telah melindung i transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-n ode enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkrip si memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data B3.b dalam Transit	Anda telah melindung i transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
Data B3.b dalam Transit	Anda telah melindung i transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data B3.b dalam Transit	Anda telah melindung i transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Data B3.b dalam Transit	Anda telah melindung i transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	s3- bucket-ssl-request s-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data B3.b dalam Transit	Anda telah melindung i transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.
Data B3.b dalam Transit	Anda telah melindung i transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data B3.b dalam Transit	Anda telah melindung i transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
Data B3.b dalam Transit	Anda telah melindung i transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSear ch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerluka n gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data B3.b dalam Transit	Anda telah melindung i transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
Data B3.b dalam Transit	Anda telah melindung i transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data B3.b dalam Transit	Anda telah melindung i transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data B3.b dalam Transit	Anda telah melindungi transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data B3.b dalam Transit	Anda telah melindung i transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data B3.b dalam Transit	Anda telah melindung i transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
Data B3.b dalam Transit	Anda telah melindung i transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data B3.b dalam Transit	Anda telah melindungi transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data B3.b dalam Transit	Anda telah melindung i transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	sagemaker-notebook -no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data B3.b dalam Transit	Anda telah melindung i transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data B3.b dalam Transit	Anda telah melindung i transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/ 0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data B3.b dalam Transit	Anda telah melindungi transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data B3.b dalam Transit	Anda telah melindungi transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data B3.b dalam Transit	Anda telah melindungi transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data B3.b dalam Transit	Anda telah melindungi transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data B3.b dalam Transit	Anda telah melindungi transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Data B3.b dalam Transit	Anda telah melindungi transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Data B3.b dalam Transit	Anda telah melindung i transit data yang penting untuk pengoperasian fungsi penting. Ini termasuk transfer data ke pihak ketiga.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
B3.c Data Tersimpan	Anda telah melindung i data yang disimpan yang penting untuk pengoperasian fungsi penting.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrai l jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B3.c Data Tersimpan	Anda telah melindungi data yang disimpan yang penting untuk pengoperasian fungsi penting.	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
B3.c Data Tersimpan	Anda telah melindungi data yang disimpan yang penting untuk pengoperasian fungsi penting.	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B3.c Data Tersimpan	Anda telah melindung i data yang disimpan yang penting untuk pengoperasian fungsi penting.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
B3.c Data Tersimpan	Anda telah melindung i data yang disimpan yang penting untuk pengoperasian fungsi penting.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
B3.c Data Tersimpan	Anda telah melindung i data yang disimpan yang penting untuk pengoperasian fungsi penting.	elasticsearch-encr ypted-at-rest	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk domain OpenSearc h Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B3.c Data Tersimpan	Anda telah melindung i data yang disimpan yang penting untuk pengoperasian fungsi penting.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
B3.c Data Tersimpan	Anda telah melindung i data yang disimpan yang penting untuk pengoperasian fungsi penting.	rds-snapshot-encry pted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B3.c Data Tersimpan	Anda telah melindungi data yang disimpan yang penting untuk pengoperasian fungsi penting.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B3.c Data Tersimpan	Anda telah melindungi data yang disimpan yang penting untuk pengoperasian fungsi penting.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B3.c Data Tersimpan	Anda telah melindung i data yang disimpan yang penting untuk pengoperasian fungsi penting.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
B3.c Data Tersimpan	Anda telah melindung i data yang disimpan yang penting untuk pengoperasian fungsi penting.	sagemaker-endpoint -configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B3.c Data Tersimpan	Anda telah melindungi data yang disimpan yang penting untuk pengoperasian fungsi penting.	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B3.c Data Tersimpan	Anda telah melindungi data yang disimpan yang penting untuk pengoperasian fungsi penting.	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
B3.c Data Tersimpan	Anda telah melindungi data yang disimpan yang penting untuk pengoperasian fungsi penting.	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B3.c Data Tersimpan	Anda telah melindungi data yang disimpan yang penting untuk pengoperasian fungsi penting.	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B3.c Data Tersimpan	Anda telah melindungi data yang disimpan yang penting untuk pengoperasian fungsi penting.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B3.c Data Tersimpan	Anda telah melindungi data yang disimpan yang penting untuk pengoperasian fungsi penting.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B3.c Data Tersimpan	Anda telah melindungi data yang disimpan yang penting untuk pengoperasian fungsi penting.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan cadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B3.c Data Tersimpan	Anda telah melindung i data yang disimpan yang penting untuk pengoperasian fungsi penting.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B3.c Data Tersimpan	Anda telah melindungi data yang disimpan yang penting untuk pengoperasian fungsi penting.	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B3.c Data Tersimpan	Anda telah melindung i data yang disimpan yang penting untuk pengoperasian fungsi penting.	efs-in-backup-plan	Untuk membantu proses pencadang an data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B3.c Data Tersimpan	Anda telah melindungi data yang disimpan yang penting untuk pengoperasian fungsi penting.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B3.c Data Tersimpan	Anda telah melindung i data yang disimpan yang penting untuk pengoperasian fungsi penting.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B3.c Data Tersimpan	Anda telah melindungi data yang disimpan yang penting untuk pengoperasian fungsi penting.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B3.c Data Tersimpan	Anda telah melindung i data yang disimpan yang penting untuk pengoperasian fungsi penting.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B3.c Data Tersimpan	Anda telah melindung i data yang disimpan yang penting untuk pengoperasian fungsi penting.	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relationa l Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindun gan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersedi aan untuk aplikasi Anda.
B3.c Data Tersimpan	Anda telah melindung i data yang disimpan yang penting untuk pengoperasian fungsi penting.	s3- bucket-default-loc k-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B3.c Data Tersimpan	Anda telah melindungi data yang disimpan yang penting untuk pengoperasian fungsi penting.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B3.c Data Tersimpan	Anda telah melindungi data yang disimpan yang penting untuk pengoperasian fungsi penting.	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
B3.c Data Tersimpan	Anda telah melindungi data yang disimpan yang penting untuk pengoperasian fungsi penting.	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	alb-http-drop-invalid-Header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSear ch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerluka n gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimalkan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimalkan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	s3- account-level-publ ic-access -blok-per iodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	sagemaker-notebook -no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemelihar aan kapasitas dan ketersediaan yang memadai. Penyeimba ng beban secara berkala mengirimk an ping, mencoba koneksi, atau mengirim permintaa n untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastika n bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/ tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyarat an throughput Anda. Aturan ini menghasil kan peringatan ketika throughpu t mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentas e WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimalkan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimalkan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimalkan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	lambda-concurrency-check	Aturan ini memastikan bahwa batas tinggi dan rendah konkurensi fungsi Lambda ditetapkan. Ini dapat membantu dalam mendasarkan jumlah permintaan yang dilayani oleh fungsi Anda pada waktu tertentu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relationa l Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindun gan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersedi aan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersedi aan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplika si data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastru ktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutk an operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	s3- bucket-default-loc k-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimalkan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.a Aman dengan Desain	Anda merancang keamanan ke dalam jaringan dan sistem informasi yang mendukung pengoperasian fungsi-fungsi penting. Anda meminimal kan permukaan serangan mereka dan memastikan bahwa pengoperasian fungsi penting tidak boleh terpengaruh oleh eksploitasi kerentanan tunggal apa pun.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.b Konfigurasi Aman	Anda mengkonfigurasi jaringan dan sistem informasi dengan aman yang mendukung pengoperasian fungsi-fungsi penting.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.b Konfigurasi Aman	Anda mengkonfi gurasi jaringan dan sistem informasi dengan aman yang mendukung pengoperasian fungsi-fungsi penting.	ec2- -periksa managedinstance-pa tch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.b Konfigurasi Aman	Anda mengkonfigurasi jaringan dan sistem informasi dengan aman yang mendukung pengoperasian fungsi-fungsi penting.	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.b Konfigurasi Aman	Anda mengkonfigurasi jaringan dan sistem informasi dengan aman yang mendukung pengoperasian fungsi-fungsi penting.	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.c Manajemen Aman	Anda mengelola jaringan dan sistem informasi organisasi Anda yang mendukung pengoperasian fungsi-fungsi penting untuk mengaktifkan dan memelihara keamanan.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.c Manajemen Aman	Anda mengelola jaringan dan sistem informasi organisasi Anda yang mendukung pengoperasian fungsi-fungsi penting untuk mengaktifkan dan memelihara keamanan.	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.c Manajemen Aman	Anda mengelola jaringan dan sistem informasi organisasi Anda yang mendukung pengoperasian fungsi-fungsi penting untuk mengaktifkan dan memelihara keamanan.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.d. Manajemen Kerentanan	Anda mengelola kerentanan yang diketahui dalam jaringan dan sistem informasi Anda untuk mencegah dampak buruk pada fungsi penting.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.d. Manajemen Kerentanan	Anda mengelola kerentanan yang diketahui dalam jaringan dan sistem informasi Anda untuk mencegah dampak buruk pada fungsi penting.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.d. Manajemen Kerentanan	Anda mengelola kerentanan yang diketahui dalam jaringan dan sistem informasi Anda untuk mencegah dampak buruk pada fungsi penting.	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.d. Manajemen Kerentanan	Anda mengelola kerentanan yang diketahui dalam jaringan dan sistem informasi Anda untuk mencegah dampak buruk pada fungsi penting.	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.d. Manajemen Kerentanan	Anda mengelola kerentanan yang diketahui dalam jaringan dan sistem informasi Anda untuk mencegah dampak buruk pada fungsi penting.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B4.d. Manajemen Kerentanan	Anda mengelola kerentanan yang diketahui dalam jaringan dan sistem informasi Anda untuk mencegah dampak buruk pada fungsi penting.	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Desain B5.b untuk Ketahanan	Anda merancang jaringan dan sistem informasi yang mendukung fungsi penting Anda agar tahan terhadap insiden keamanan cyber. Sistem dipisahkan dengan tepat dan keterbatasan sumber daya dikurangi.	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Desain B5.b untuk Ketahanan	Anda merancang jaringan dan sistem informasi yang mendukung fungsi penting Anda agar tahan terhadap insiden keamanan cyber. Sistem dipisahkan dengan tepat dan keterbatasan sumber daya dikurangi.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Desain B5.b untuk Ketahanan	Anda merancang jaringan dan sistem informasi yang mendukung fungsi penting Anda agar tahan terhadap insiden keamanan cyber. Sistem dipisahkan dengan tepat dan keterbata san sumber daya dikurangi.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B5.c Backup	Anda menyimpan cadangan data dan informasi saat ini yang dapat diakses dan diamankan yang diperlukan untuk memulihkan operasi fungsi penting Anda	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B5.c Backup	Anda menyimpan cadangan data dan informasi saat ini yang dapat diakses dan diamankan yang diperlukan untuk memulihkan operasi fungsi penting Anda	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan cadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B5.c Backup	Anda menyimpan cadangan data dan informasi saat ini yang dapat diakses dan diamankan yang diperlukan untuk memulihkan operasi fungsi penting Anda	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B5.c Backup	Anda menyimpan cadangan data dan informasi saat ini yang dapat diakses dan diamankan yang diperlukan untuk memulihkan operasi fungsi penting Anda	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B5.c Backup	Anda menyimpan cadangan data dan informasi saat ini yang dapat diakses dan diamankan yang diperlukan untuk memulihkan operasi fungsi penting Anda	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B5.c Backup	Anda menyimpan cadangan data dan informasi saat ini yang dapat diakses dan diamankan yang diperlukan untuk memulihkan operasi fungsi penting Anda	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B5.c Backup	Anda menyimpan cadangan data dan informasi saat ini yang dapat diakses dan diamankan yang diperlukan untuk memulihkan operasi fungsi penting Anda	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B5.c Backup	Anda menyimpan cadangan data dan informasi saat ini yang dapat diakses dan diamankan yang diperlukan untuk memulihkan operasi fungsi penting Anda	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B5.c Backup	Anda menyimpan cadangan data dan informasi saat ini yang dapat diakses dan diamankan yang diperlukan untuk memulihkan operasi fungsi penting Anda	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
B5.c Backup	Anda menyimpan cadangan data dan informasi saat ini yang dapat diakses dan diamankan yang diperlukan untuk memulihkan operasi fungsi penting Anda	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Cakupan Pemantauan C1.a	Sumber data yang Anda sertakan dalam pemantauan memungkinkan identifikasi peristiwa keamanan secara tepat waktu yang dapat memengaruhi pengoperasian fungsi penting Anda.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Cakupan Pemantauan C1.a	Sumber data yang Anda sertakan dalam pemantauan memungkinkan identifikasi peristiwa keamanan secara tepat waktu yang dapat memengaruhi pengoperasian fungsi penting Anda.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Cakupan Pemantauan C1.a	Sumber data yang Anda sertakan dalam pemantauan memungkinkan identifikasi peristiwa keamanan secara tepat waktu yang dapat memengaruhi pengoperasian fungsi penting Anda.	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
Cakupan Pemantauan C1.a	Sumber data yang Anda sertakan dalam pemantauan memungkinkan identifikasi peristiwa keamanan secara tepat waktu yang dapat memengaruhi pengoperasian fungsi penting Anda.	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Cakupan Pemantauan C1.a	Sumber data yang Anda sertakan dalam pemantauan memungkinkan identifikasi peristiwa keamanan secara tepat waktu yang dapat memengaruhi pengoperasian fungsi penting Anda.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Cakupan Pemantauan C1.a	Sumber data yang Anda sertakan dalam pemantauan memungkinkan identifikasi peristiwa keamanan secara tepat waktu yang dapat memengaruhi pengoperasian fungsi penting Anda.	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Cakupan Pemantauan C1.a	Sumber data yang Anda sertakan dalam pemantauan memungkinkan identifikasi peristiwa keamanan secara tepat waktu yang dapat memengaruhi pengoperasian fungsi penting Anda.	lambda-concurrency-check	Aturan ini memastikan bahwa batas tinggi dan rendah konkurensi fungsi Lambda ditetapkan. Ini dapat membantu dalam mendasarkan jumlah permintaan yang dilayani oleh fungsi Anda pada waktu tertentu.
Cakupan Pemantauan C1.a	Sumber data yang Anda sertakan dalam pemantauan memungkinkan identifikasi peristiwa keamanan secara tepat waktu yang dapat memengaruhi pengoperasian fungsi penting Anda.	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Cakupan Pemantauan C1.a	Sumber data yang Anda sertakan dalam pemantauan memungkinkan identifikasi peristiwa keamanan secara tepat waktu yang dapat memengaruhi pengoperasian fungsi penting Anda.	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Cakupan Pemantauan C1.a	Sumber data yang Anda sertakan dalam pemantauan memungkinkan identifikasi peristiwa keamanan secara tepat waktu yang dapat memengaruhi pengoperasian fungsi penting Anda.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Cakupan Pemantauan C1.a	Sumber data yang Anda sertakan dalam pemantauan memungkinkan identifikasi peristiwa keamanan secara tepat waktu yang dapat memengaruhi pengoperasian fungsi penting Anda.	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
C1.b Mengamankan Log	Anda menyimpan data pencatatan dengan aman dan memberikan akses baca hanya ke akun yang membutuhk an bisnis. Tidak ada karyawan yang perlu memodifikasi atau menghapus data pencatatan dalam periode retensi yang disepakati, setelah itu harus dihapus.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediak an metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinc i untuk permintaa n yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
C1.b Mengamankan Log	Anda menyimpan data pencatatan dengan aman dan memberikan akses baca hanya ke akun yang membutuhk an bisnis. Tidak ada karyawan yang perlu memodifikasi atau menghapus data pencatatan dalam periode retensi yang disepakati, setelah itu harus dihapus.	s3- bucket-policy-gran tee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_ bucket_policy_gran tee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs
C1.b Mengamankan Log	Anda menyimpan data pencatatan dengan aman dan memberikan akses baca hanya ke akun yang membutuhk an bisnis. Tidak ada karyawan yang perlu memodifikasi atau menghapus data pencatatan dalam periode retensi yang disepakati, setelah itu harus dihapus.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
C1.b Mengamankan Log	Anda menyimpan data pencatatan dengan aman dan memberikan akses baca hanya ke akun yang membutuhkan bisnis. Tidak ada karyawan yang perlu memodifikasi atau menghapus data pencatatan dalam periode retensi yang disepakati, setelah itu harus dihapus.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
C1.b Mengamankan Log	Anda menyimpan data pencatatan dengan aman dan memberikan akses baca hanya ke akun yang membutuhkan bisnis. Tidak ada karyawan yang perlu memodifikasi atau menghapus data pencatatan dalam periode retensi yang disepakati, setelah itu harus dihapus.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
C1.b Mengamankan Log	Anda menyimpan data pencatatan dengan aman dan memberikan akses baca hanya ke akun yang membutuhk an bisnis. Tidak ada karyawan yang perlu memodifikasi atau menghapus data pencatatan dalam periode retensi yang disepakati, setelah itu harus dihapus.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
C1.b Mengamankan Log	Anda menyimpan data pencatatan dengan aman dan memberikan akses baca hanya ke akun yang membutuhk an bisnis. Tidak ada karyawan yang perlu memodifikasi atau menghapus data pencatatan dalam periode retensi yang disepakati, setelah itu harus dihapus.	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
C1.b Mengamankan Log	Anda menyimpan data pencatatan dengan aman dan memberikan akses baca hanya ke akun yang membutuhkan bisnis. Tidak ada karyawan yang perlu memodifikasi atau menghapus data pencatatan dalam periode retensi yang disepakati, setelah itu harus dihapus.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
C1.b Mengamankan Log	Anda menyimpan data pencatatan dengan aman dan memberikan akses baca hanya ke akun yang membutuhk an bisnis. Tidak ada karyawan yang perlu memodifikasi atau menghapus data pencatatan dalam periode retensi yang disepakati, setelah itu harus dihapus.	iam-user-no-policies-periksa	Aturan ini memastika n kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapka n hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
C1.b Mengamankan Log	Anda menyimpan data pencatatan dengan aman dan memberikan akses baca hanya ke akun yang membutuhk an bisnis. Tidak ada karyawan yang perlu memodifikasi atau menghapus data pencatatan dalam periode retensi yang disepakati, setelah itu harus dihapus.	iam-user-unused-cr edentials-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharus kan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
C1.b Mengamankan Log	Anda menyimpan data pencatatan dengan aman dan memberikan akses baca hanya ke akun yang membutuhk an bisnis. Tidak ada karyawan yang perlu memodifikasi atau menghapus data pencatatan dalam periode retensi yang disepakati, setelah itu harus dihapus.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
C1.c Menghasilkan Peringatan	Bukti potensi insiden keamanan yang terkandung dalam data pemantauan Anda diidentifikasi dengan andal dan memicu peringatan.	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
C1.c Menghasilkan Peringatan	Bukti potensi insiden keamanan yang terkandung dalam data pemantauan Anda diidentifikasi dengan andal dan memicu peringatan.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
C1.c Menghasilkan Peringatan	Bukti potensi insiden keamanan yang terkandung dalam data pemantauan Anda diidentifikasi dengan andal dan memicu peringatan.	s3- event-notifications-enabled	Pemberitahuan peristiwa Amazon S3 dapat memberi tahu personel terkait tentang modifikasi yang tidak disengaja atau disengaja pada objek bucket Anda. Contoh peringatan meliputi: objek baru adalah pembuatan, penghapusan objek, restorasi objek, objek yang hilang dan direplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
C1.c Menghasilkan Peringatan	Bukti potensi insiden keamanan yang terkandung dalam data pemantauan Anda diidentifikasi dengan andal dan memicu peringatan.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
C1.c Menghasilkan Peringatan	Bukti potensi insiden keamanan yang terkandung dalam data pemantauan Anda diidentifikasi dengan andal dan memicu peringatan.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
C1.c Menghasilkan Peringatan	Bukti potensi insiden keamanan yang terkandung dalam data pemantauan Anda diidentifikasi dengan andal dan memicu peringatan.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
C1.c Menghasilkan Peringatan	Bukti potensi insiden keamanan yang terkandung dalam data pemantauan Anda diidentifikasi dengan andal dan memicu peringatan.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
C1.c Menghasilkan Peringatan	Bukti potensi insiden keamanan yang terkandung dalam data pemantauan Anda diidentifikasi dengan andal dan memicu peringatan.	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
C1.c Menghasilkan Peringatan	Bukti potensi insiden keamanan yang terkandung dalam data pemantauan Anda diidentifikasi dengan andal dan memicu peringatan.	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
C1.c Menghasilkan Peringatan	Bukti potensi insiden keamanan yang terkandung dalam data pemantauan Anda diidentifikasi dengan andal dan memicu peringatan.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
C1.c Menghasilkan Peringatan	Bukti potensi insiden keamanan yang terkandung dalam data pemantauan Anda diidentifikasi dengan andal dan memicu peringatan.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
C1.c Menghasilkan Peringatan	Bukti potensi insiden keamanan yang terkandung dalam data pemantauan Anda diidentifikasi dengan andal dan memicu peringatan.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
C1.c Menghasilkan Peringatan	Bukti potensi insiden keamanan yang terkandung dalam data pemantauan Anda diidentifikasi dengan andal dan memicu peringatan.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
C1.c Menghasilkan Peringatan	Bukti potensi insiden keamanan yang terkandung dalam data pemantauan Anda diidentifikasi dengan andal dan memicu peringatan.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
C1.c Menghasilkan Peringatan	Bukti potensi insiden keamanan yang terkandung dalam data pemantauan Anda diidentifikasi dengan andal dan memicu peringatan.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
C1.c Menghasilkan Peringatan	Bukti potensi insiden keamanan yang terkandung dalam data pemantauan Anda diidentifikasi dengan andal dan memicu peringatan.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
C1.d Mengidentifikasi Insiden Keamanan	Anda mengontek stualisasikan peringatan dengan pengetahuan tentang ancaman dan sistem Anda, untuk mengidentifikasi insiden keamanan yang memerlukan beberapa bentuk respons.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
C1.d Mengidentifikasi Insiden Keamanan	Anda mengontek stualisasikan peringatan dengan pengetahuan tentang ancaman dan sistem Anda, untuk mengidentifikasi insiden keamanan yang memerlukan beberapa bentuk respons.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Alat dan Keterampilan Pemantauan C1.e	Memantau keterampilan, alat, dan peran staf, termasuk apa pun yang dialihdayakan, harus mencerminkan persyaratan tata kelola dan pelaporan, ancaman yang diharapkan, dan kompleksitas data jaringan atau sistem yang perlu mereka gunakan. Staf pemantauan memiliki pengetahuan tentang fungsi-fungsi penting yang perlu mereka lindungi.	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Alat dan Keterampilan Pemantauan C1.e	Memantau keterampilan, alat, dan peran staf, termasuk apa pun yang dialihdayakan, harus mencermin kan persyaratan tata kelola dan pelaporan, ancaman yang diharapkan, dan kompleksitas data jaringan atau sistem yang perlu mereka gunakan. Staf pemantauan memiliki pengetahuan tentang fungsi-fungsi penting yang perlu mereka lindungi.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Alat dan Keterampilan Pemantauan C1.e	Memantau keterampilan, alat, dan peran staf, termasuk apa pun yang dialihdayakan, harus mencerminkan persyaratan tata kelola dan pelaporan, ancaman yang diharapkan, dan kompleksitas data jaringan atau sistem yang perlu mereka gunakan. Staf pemantauan memiliki pengetahuan tentang fungsi-fungsi penting yang perlu mereka lindungi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Kelainan Sistem C2.a untuk Deteksi Serangan	Anda mendefinisikan contoh kelainan dalam perilaku sistem yang menyediakan cara praktis untuk mendeteksi aktivitas berbahaya yang sulit diidentifikasi.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
Kelainan Sistem C2.a untuk Deteksi Serangan	Anda mendefinisikan contoh kelainan dalam perilaku sistem yang menyediakan cara praktis untuk mendeteksi aktivitas berbahaya yang sulit diidentifikasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
D1.c Menguji dan Berolahraga	Organisasi Anda melakukan latihan untuk menguji rencana respons, menggunakan insiden masa lalu yang memengaruhi organisasi Anda (dan lainnya), dan skenario yang mengacu pada kecerdasan ancaman dan penilaian risiko Anda.	response-plan-exists-maintained (Pemeriksaan Proses)	Memastikan rencana respons insiden dibuat, dipelihara, dan didistribusikan kepada personel yang bertanggung jawab. Memiliki rencana respons yang diperbarui dan didokumentasikan secara formal dapat membantu memastikan personel respons memahami peran, tanggung jawab, dan proses yang harus diikuti selama insiden.
D1.c Menguji dan Berolahraga	Organisasi Anda melakukan latihan untuk menguji rencana respons, menggunakan insiden masa lalu yang memengaruhi organisasi Anda (dan lainnya), dan skenario yang mengacu pada kecerdasan ancaman dan penilaian risiko Anda.	response-plan-tested (Pemeriksaan Proses)	Pastikan respon Insiden dan rencana pemulihan diuji. Ini dapat membantu dalam memahami apakah rencana Anda akan efektif selama insiden dan jika ada celah atau pembaruan yang perlu ditangani.

Templat

Template ini tersedia di GitHub: Praktik Terbaik Operasional untuk Kerangka Penilaian Cyber NCSC.

Praktik Terbaik Operasional untuk Jaringan dan Layanan Pengiriman Konten

Paket kesesuaian ini berisi AWS Config aturan berdasarkan Jaringan dan Layanan Pengiriman Konten. Untuk informasi selengkapnya, lihat Jaringan dan Pengiriman Konten di AWS. Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Jaringan dan Layanan Pengiriman Konten.

Praktik Terbaik Operasional untuk NIST 800-53 rev 4

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini menyediakan contoh pemetaan antara aturan NIST 800-53 dan Config terkelola AWS . Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan berhubungan dengan satu atau beberapa kontrol NIST 800-53. Kontrol NIST 800-53 dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

Paket Kesesuaian ini divalidasi oleh AWS Security Assurance Services LLC (AWS SAS), yang merupakan tim dari Payment Card Industry Qualified Security Assesors (QSAs), HITRUST Certified Common Security Framework Practitioners (CCSFPs), dan profesional kepatuhan yang disertifikasi untuk memberikan panduan dan penilaian untuk berbagai kerangka kerja industri. AWS Profesional SAS merancang Paket Kesesuaian ini untuk memungkinkan pelanggan menyelaraskan ke subset NIST 800-53.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	secretsmanager-scheduled-rotation-success-periksa	Aturan ini memastikan bahwa AWS rahasia Secrets Manager telah berhasil diputar sesuai dengan jadwal rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode di mana rahasia aktif, dan berpotensi mengurangi dampak bisnis jika dikompromikan.
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
			paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan Centers for Internet Security (CIS) AWS Foundations Benchmark untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar),

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
			RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung pengelolaan akun sistem informasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (3)	Sistem informasi secara otomatis menonaktifkan akun yang tidak aktif setelah [Penugasan: periode waktu yang ditentukan organisasi].	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikas i, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisas i].	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikasi, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisasi].	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikasi, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisasi].	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikasi, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisasi].	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikasi, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisasi].	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua Wilayah AWS ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS melluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikasi, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisasi].	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikasi, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisasi].	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (4)	Sistem informasi secara otomatis mengaudit pembuatan akun, modifikasi, mengaktifkan, menonaktifkan, dan menghapus tindakan, dan memberi tahu [Penugasan: personel atau peran yang ditentukan organisasi].	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (12) (a)	Organisasi: a. Memantau akun sistem informasi untuk [Penugasan: penggunaan atipikal yang ditentukan organisasi].	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (12) (a)	Organisasi: a. Memantau akun sistem informasi untuk [Penugasan: penggunaan atipikal yang ditentukan organisasi].	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (f)	Organisasi: f. Membuat, mengaktifkan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisasi].	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (f)	Organisasi: f. Membuat, mengaktif kan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisas i].	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifik asi berdasark an kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyatakan oleh NIST SP 800-63 dan Centers for Internet Security (CIS) AWS Foundations Benchmark untuk kekuatan kata sandi. Aturan ini memungkin kan Anda untuk mengatur secara opsional RequireUp percaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar),

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
			RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (f)	Organisasi: f. Membuat, mengaktif kan, memodifikasi, menonaktifkan, dan menghapus akun sistem informasi sesuai dengan [Penugasan: prosedur atau kondisi yang ditentukan organisas i].	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
AC-2 (g)	Organisasi: g. Memantau penggunaan akun sistem informasi.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	root-account-mfa-e nabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindun gan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyaratan manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	secretsmanager-scheduled-rotation-success-periksa	Aturan ini memastikan bahwa AWS rahasia Secrets Manager telah berhasil diputar sesuai dengan jadwal rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode di mana rahasia aktif, dan berpotensi mengurangi dampak bisnis jika dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-user-group-mem bership-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastika n pengguna adalah anggota setidaknya satu grup. Mengizink an pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifik asi berdasark an kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyatakan oleh NIST SP 800-63 dan Centers for Internet Security (CIS) AWS Foundations Benchmark untuk kekuatan kata sandi. Aturan ini memungkin kan Anda untuk mengatur secara opsional RequireUp percaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar),

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
			RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastika n kunci akses IAM diputar sebagaima na ditentukan oleh kebijakan organisas i. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurang i dampak bisnis jika kunci dikompromikan. Aturan ini memerluka n nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengotent ikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-2 (j)	Organisasi: j. Ulasan akun untuk kepatuhan dengan persyarat an manajemen akun [Penugasan: frekuensi yang ditentukan organisasi].	iam-user-no-policies-periksa	Aturan ini memastika n kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapka n hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	s3- -blok account-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengotent ikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-3	Sistem informasi memberlakukan otorisasi yang disetujui untuk akses logis ke informasi dan sumber daya sistem sesuai dengan kebijakan kontrol akses yang berlaku.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubungan berdasarkan [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisasi].	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	s3- -blok account-l evel-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	sagemaker-notebook -no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	acm-certificate-ex piration-check	Pastikan integritas jaringan dilindungi dengan memastika n sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExp iration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSear ch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerluka n gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-4	Sistem informasi memberlakukan otorisasi yang disetujui untuk mengendalikan aliran informasi dalam sistem dan antara sistem yang saling berhubung an berdasark an [Penugasan: kebijakan kontrol aliran informasi yang ditentukan organisas i].	internet-gateway-a uthorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirk an ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-5c	Organisasi: c. Mendefinisikan otorisasi akses sistem informasi untuk mendukung pemisahan tugas.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengotent ikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-5c	Organisasi: c. Mendefinisikan otorisasi akses sistem informasi untuk mendukung pemisahan tugas.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-5c	Organisasi: c. Mendefinisikan otorisasi akses sistem informasi untuk mendukung pemisahan tugas.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-5c	Organisasi: c. Mendefinisikan otorisasi akses sistem informasi untuk mendukung pemisahan tugas.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	s3- -blok account-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild. Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengotent ikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifka n untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-6	Organisasi menggunakan prinsip hak istimewa paling sedikit, hanya memungkinkan akses resmi untuk pengguna (atau proses yang bertindak atas nama pengguna) yang diperlukan untuk menyelesaikan tugas yang diberikan sesuai dengan misi organisasi dan fungsi bisnis.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-6 (10)	Sistem informasi mencegah pengguna yang tidak memiliki hak istimewa untuk menjalankan fungsi istimewa untuk menyertakan menonaktifkan, menghindari, atau mengubah pengamanan keamanan/penanggulangan yang diterapkan.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-17 (1)	Sistem informasi memantau dan mengontrol metode akses jarak jauh.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-17 (2)	Sistem informasi menerapkan mekanisme kriptografi untuk melindungi kerahasiaan dan integritas sesi akses jarak jauh.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
AC-17 (2)	Sistem informasi menerapkan mekanisme kriptografi untuk melindungi kerahasiaan dan integritas sesi akses jarak jauh.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-17 (2)	Sistem informasi menerapkan mekanisme kriptografi untuk melindungi kerahasiaan dan integritas sesi akses jarak jauh.	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-17 (2)	Sistem informasi menerapkan mekanisme kriptografi untuk melindungi kerahasiaan dan integritas sesi akses jarak jauh.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-17 (2)	Sistem informasi menerapkan mekanisme kriptografi untuk melindungi kerahasiaan dan integritas sesi akses jarak jauh.	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
AC-17 (2)	Sistem informasi menerapkan mekanisme kriptografi untuk melindungi kerahasiaan dan integritas sesi akses jarak jauh.	alb-http-drop-invalid-Header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-17 (2)	Sistem informasi menerapkan mekanisme kriptografi untuk melindungi kerahasiaan dan integritas sesi akses jarak jauh.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
AC-17 (3)	Sistem informasi merutekan semua akses jarak jauh melalui [Penugasan: nomor yang ditentukan organisasi] titik kontrol akses jaringan terkelola.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	s3- -blok account-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AC-21 (b)	Organisasi: b. Mempekerjakan [Penugasan: mekanisme otomatis yang ditentukan organisasi atau proses manual] untuk membantu pengguna dalam membuat keputusan berbagi informasi/kolaborasi.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa-peristiwa berikut: [Penugasan: peristiwa yang dapat diaudit yang ditentukan organisasi]; d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [Penugasan: peristiwa audit yang ditentukan organisasi (bagian dari peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a.) bersama dengan frekuensi (atau situasi yang membutuhkan) audit untuk setiap peristiwa yang diidentifikasi].	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa-peristiwa berikut: [Penugasan: peristiwa yang dapat diaudit yang ditentukan organisasi]; d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [Penugasan: peristiwa audit yang ditentukan organisasi (bagian dari peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a.) bersama dengan frekuensi (atau situasi yang membutuhkan) audit untuk setiap peristiwa yang diidentifikasi].	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa-peristiwa berikut: [Penugasan: peristiwa yang dapat diaudit yang ditentukan organisasi]; d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [Penugasan: peristiwa audit yang ditentukan organisasi (bagian dari peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a.) bersama dengan frekuensi (atau situasi yang membutuhkan) audit untuk setiap peristiwa yang diidentifikasi].	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa-peristiwa berikut: [Penugasan: peristiwa yang dapat diaudit yang ditentukan organisasi]; d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [Penugasan: peristiwa audit yang ditentukan organisasi (bagian dari peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a.) bersama dengan frekuensi (atau situasi yang membutuhkan) audit untuk setiap peristiwa yang diidentifikasi].	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa-peristiwa berikut: [Penugasan: peristiwa yang dapat diaudit yang ditentukan organisasi]; d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [Penugasan: peristiwa audit yang ditentukan organisasi (bagian dari peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a.) bersama dengan frekuensi (atau situasi yang membutuhkan) audit untuk setiap peristiwa yang diidentifikasi].	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa-peristiwa berikut: [Penugasan: peristiwa yang dapat diaudit yang ditentukan organisasi]; d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [Penugasan: peristiwa audit yang ditentukan organisasi (bagian dari peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a.) bersama dengan frekuensi (atau situasi yang membutuhkan) audit untuk setiap peristiwa yang diidentifikasi].	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua Wilayah AWS ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS melluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa-peristiwa berikut: [Penugasan: peristiwa yang dapat diaudit yang ditentukan organisasi]; d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [Penugasan: peristiwa audit yang ditentukan organisasi (bagian dari peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a.) bersama dengan frekuensi (atau situasi yang membutuhkan) audit untuk setiap peristiwa yang diidentifikasi].	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa-peristiwa berikut: [Penugasan: peristiwa yang dapat diaudit yang ditentukan organisasi]; d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [Penugasan: peristiwa audit yang ditentukan organisasi (bagian dari peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a.) bersama dengan frekuensi (atau situasi yang membutuhkan) audit untuk setiap peristiwa yang diidentifikasi].	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa-peristiwa berikut: [Penugasan: peristiwa yang dapat diaudit yang ditentukan organisasi]; d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [Penugasan: peristiwa audit yang ditentukan organisasi (bagian dari peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a.) bersama dengan frekuensi (atau situasi yang membutuhkan) audit untuk setiap peristiwa yang diidentifikasi].	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa-peristiwa berikut: [Penugasan: peristiwa yang dapat diaudit yang ditentukan organisasi]; d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [Penugasan: peristiwa audit yang ditentukan organisasi (bagian dari peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a.) bersama dengan frekuensi (atau situasi yang membutuhkan) audit untuk setiap peristiwa yang diidentifikasi].	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-2 (a) (d)	Organisasi: a. Menentukan bahwa sistem informasi mampu mengaudit peristiwa-peristiwa berikut: [Penugasan: peristiwa yang dapat diaudit yang ditentukan organisasi]; d. Menentukan bahwa peristiwa berikut akan diaudit dalam sistem informasi: [Penugasan: peristiwa audit yang ditentukan organisasi (bagian dari peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a.) bersama dengan frekuensi (atau situasi yang membutuhkan) audit untuk setiap peristiwa yang diidentifikasi].	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua Wilayah AWS ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS melluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-3	Sistem informasi menghasilkan catatan audit yang berisi informasi yang menetapkan jenis peristiwa apa yang terjadi, kapan peristiwa itu terjadi, di mana peristiwa itu terjadi, sumber peristiwa, hasil peristiwa, dan identitas setiap individu atau subjek yang terkait dengan peristiwa tersebut.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-6 (1) (3)	(1) Organisas i menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisas i untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisas i menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-6 (1) (3)	(1) Organisasi menggunakan mekanisme otomatis untuk menginteg rasikan tinjauan audit, analisis, dan proses pelaporan untuk mendukung proses organisasi untuk penyelidi kan dan respons terhadap kegiatan yang mencuriga kan. (3) Organisasi menganalisis dan mengkorelasikan catatan audit di berbagai repositori untuk mendapatkan kesadaran situasional di seluruh organisasi.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-7 (1)	Sistem informasi menyediakan kemampuan untuk memproses catatan audit untuk peristiwa yang menarik berdasarkan [Penugasan: bidang audit yang ditentukan organisasi dalam catatan audit].	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-7 (1)	Sistem informasi menyediakan kemampuan untuk memproses catatan audit untuk peristiwa yang menarik berdasarkan [Penugasan: bidang audit yang ditentuka n organisasi dalam catatan audit].	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
AU-9	Sistem informasi melindungi informasi audit dan alat audit dari akses, modifikas i, dan penghapusan yang tidak sah.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrai l jejak Anda.
AU-9	Sistem informasi melindungi informasi audit dan alat audit dari akses, modifikas i, dan penghapusan yang tidak sah.	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-9 (2)	Sistem informasi mencadangkan catatan audit [Penugasan: frekuensi yang ditentukan organisasi] ke sistem atau komponen sistem yang berbeda secara fisik dari sistem atau komponen yang diaudit.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-11	Organisasi menyimpan catatan audit untuk [Penugasan: periode waktu yang ditentukan organisasi yang konsisten dengan kebijakan penyimpanan catatan] untuk memberikan dukungan untuk after-the-fact investigasi insiden keamanan dan untuk memenuhi persyaratan penyimpanan informasi peraturan dan organisasi.	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di [Penugasan: komponen sistem informasi yang ditentukan organisasi]; c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di [Penugasan: komponen sistem informasi yang ditentukan organisasi]; c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di [Penugasan: komponen sistem informasi yang ditentukan organisasi]; c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di [Penugasan: komponen sistem informasi yang ditentukan organisasi]; c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di [Penugasan: komponen sistem informasi yang ditentukan organisasi]; c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di [Penugasan: komponen sistem informasi yang ditentukan organisasi]; c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di [Penugasan: komponen sistem informasi yang ditentukan organisasi]; c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua Wilayah AWS ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS melluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di [Penugasan: komponen sistem informasi yang ditentukan organisasi]; c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di [Penugasan: komponen sistem informasi yang ditentukan organisasi]; c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di [Penugasan: komponen sistem informasi yang ditentukan organisasi]; c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
AU-12 (a) (c)	Sistem informasi : a. Menyediakan kemampuan pembuatan catatan audit untuk peristiwa yang dapat diaudit yang didefinisikan dalam AU-2 a. di [Penugasan: komponen sistem informasi yang ditentukan organisasi]; c. Menghasilkan catatan audit untuk peristiwa yang didefinisikan dalam AU-2 d. dengan konten yang ditentukan dalam AU-3.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantaua n berkelanjutan dan menerapkan program pemantauan berkelanj utan yang meliputi: a. Pembentuk an [Penugasa n: metrik yang ditentukan organisas i] untuk dipantau; b. Pembentuk an [Penugasan: frekuensi yang ditentukan organisas i] untuk pemantaua n dan [Penugasa n: frekuensi yang ditentukan organisas i] untuk penilaian yang mendukung pemantauan tersebut	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantaua n berkelanjutan dan menerapkan program pemantauan berkelanj utan yang meliputi: a. Pembentuk an [Penugasa n: metrik yang ditentukan organisas i] untuk dipantau; b. Pembentuk an [Penugasan: frekuensi yang ditentukan organisas i] untuk pemantaua n dan [Penugasa n: frekuensi yang ditentukan organisas i] untuk penilaian yang mendukung pemantauan tersebut.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantaua n berkelanjutan dan menerapkan program pemantauan berkelanj utan yang meliputi: a. Pembentuk an [Penugasa n: metrik yang ditentukan organisas i] untuk dipantau; b. Pembentuk an [Penugasan: frekuensi yang ditentukan organisas i] untuk pemantaua n dan [Penugasa n: frekuensi yang ditentukan organisas i] untuk penilaian yang mendukung pemantauan tersebut.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantauan berkelanjutan dan menerapkan program pemantauan berkelanjutan yang meliputi: a. Pembentukan [Penugasan: metrik yang ditentukan organisasi] untuk dipantau; b. Pembentukan [Penugasan: frekuensi yang ditentukan organisasi] untuk pemantauan dan [Penugasan: frekuensi yang ditentukan organisasi] untuk penilaian yang mendukung pemantauan tersebut.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantaua n berkelanjutan dan menerapkan program pemantauan berkelanj utan yang meliputi: a. Pembentuk an [Penugasa n: metrik yang ditentukan organisas i] untuk dipantau; b. Pembentuk an [Penugasan: frekuensi yang ditentukan organisas i] untuk pemantaua n dan [Penugasa n: frekuensi yang ditentukan organisas i] untuk penilaian yang mendukung pemantauan tersebut.	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CA-7 (a) (b)	Organisasi mengembangkan strategi pemantaua n berkelanjutan dan menerapkan program pemantauan berkelanj utan yang meliputi: a. Pembentuk an [Penugasa n: metrik yang ditentukan organisas i] untuk dipantau; b. Pembentuk an [Penugasan: frekuensi yang ditentukan organisas i] untuk pemantaua n dan [Penugasa n: frekuensi yang ditentukan organisas i] untuk penilaian yang mendukung pemantauan tersebut.	rds-enhanced-monit oring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberika n visibilitas terperinc i ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpan an Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitorin g mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigurasi dasar saat ini dari sistem informasi.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	ec2- volume-inuse-check	Aturan ini memastika n bahwa volume Amazon Elastic Block Store yang dilampirk an ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentika n, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigurasi dasar saat ini dari sistem informasi.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CM-2	Organisasi mengembangkan, mendokumentasikan, dan memelihara di bawah kontrol konfigurasi, konfigura si dasar saat ini dari sistem informasi.	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomen dasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaa n enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CM-7 (a)	Organisasi: a. Mengkonfigurasi sistem informasi untuk hanya menyediakan kemampuan penting.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CM-7 (a)	Organisasi: a. Mengkonfigurasi sistem informasi untuk hanya menyediakan kemampuan penting.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CM-8 (1)	Organisasi memperbarui inventaris komponen sistem informasi sebagai bagian integral dari instalasi komponen, penghapusan, dan pembaruan sistem informasi.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CM-8 (3) (a)	Organisasi: a. Menggunakan mekanisme otomatis [Penugasan: frekuensi yang ditentuka n organisasi] untuk mendeteks i keberadaan komponen perangkat keras, perangkat lunak, dan firmware yang tidak sah dalam sistem informasi	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CM-8 (3) (a)	Organisasi: a. Menggunakan mekanisme otomatis [Penugasan: frekuensi yang ditentuka n organisasi] untuk mendeteks i keberadaan komponen perangkat keras, perangkat lunak, dan firmware yang tidak sah dalam sistem informasi	ec2- -periksa managedinstance-as sociation-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventari s platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CM-8 (3) (a)	Organisasi: a. Menggunakan mekanisme otomatis [Penugasan: frekuensi yang ditentuka n organisasi] untuk mendeteks i keberadaan komponen perangkat keras, perangkat lunak, dan firmware yang tidak sah dalam sistem informasi	ec2- -periksa managedinstance-pa tch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan pencadangan informasi tingkat sistem yang terkandung dalam sistem informasi [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan].	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan pencadangan informasi tingkat sistem yang terkandung dalam sistem informasi [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan].	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan cadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan pencadangan informasi tingkat sistem yang terkandung dalam sistem informasi [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan].	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan pencadangan informasi tingkat sistem yang terkandung dalam sistem informasi [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan].	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan pencadangan informasi tingkat sistem yang terkandung dalam sistem informasi [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan].	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan pencadangan informasi tingkat sistem yang terkandung dalam sistem informasi [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan].	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan pencadangan informasi tingkat sistem yang terkandung dalam sistem informasi [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan].	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CP-9 (b)	Organisasi: b. Melakukan pencadangan informasi tingkat sistem yang terkandung dalam sistem informasi [Penugasan: frekuensi yang ditentukan organisasi yang konsisten dengan waktu pemulihan dan tujuan titik pemulihan].	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	rds-cluster-multi-az-diaktifkan	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan cadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
CP-10	Organisasi menyediakan pemulihan dan rekonstitusi sistem informasi ke negara yang diketahui setelah gangguan, kompromi, atau kegagalan.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relational Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
IA-2	Sistem informasi secara unik mengidentifikasi dan mengotentikasi pengguna organisasi (atau proses yang bertindak atas nama pengguna organisasi).	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan Centers for Internet Security (CIS) AWS Foundations Benchmark untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar),

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
			RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
IA-2 (1) (11)	(1) Sistem informasi menerapkan otentikasi multifaktor untuk akses jaringan ke akun istimewa. (11) Sistem informasi menerapkan otentikasi multifaktor untuk akses jarak jauh ke akun istimewa dan non-hak istimewa sehingga salah satu faktor disediakan oleh perangkat yang terpisah dari sistem yang mendapatkan akses dan perangkat memenuhi [Penugasan: kekuatan persyaratan mekanisme yang ditentukan organisasi].	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
IA-2 (1) (11)	(1) Sistem informasi menerapkan otentikasi multifaktor untuk akses jaringan ke akun istimewa. (11) Sistem informasi menerapkan otentikasi multifaktor untuk akses jarak jauh ke akun istimewa dan non-hak istimewa sehingga salah satu faktor disediakan oleh perangkat yang terpisah dari sistem yang mendapatkan akses dan perangkat memenuhi [Penugasan: kekuatan persyaratan mekanisme yang ditentukan organisasi].	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
IA-2 (1) (2) (11)	(1) Sistem informasi menerapkan otentikasi multifaktor untuk akses jaringan ke akun istimewa. (2) Sistem informasi menerapkan otentikasi multifaktor untuk akses jaringan ke akun yang tidak memiliki hak istimewa. (11) Sistem informasi menerapkan otentikasi multifaktor untuk akses jarak jauh ke akun istimewa dan non-hak istimewa sehingga salah satu faktor disediakan oleh perangkat yang terpisah dari sistem yang mendapatkan akses dan perangkat memenuhi [Penugasan: kekuatan persyaratan mekanisme yang ditentukan organisasi].	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
IA-2 (1) (2) (11)	(1) Sistem informasi menerapkan otentikasi multifaktor untuk akses jaringan ke akun istimewa. (2) Sistem informasi menerapkan otentikasi multifaktor untuk akses jaringan ke akun yang tidak memiliki hak istimewa. (11) Sistem informasi menerapkan otentikasi multifaktor untuk akses jarak jauh ke akun istimewa dan non-hak istimewa sehingga salah satu faktor disediakan oleh perangkat yang terpisah dari sistem yang mendapatkan akses dan perangkat memenuhi [Penugasan: kekuatan persyaratan mekanisme yang ditentukan organisasi].	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
IA-5 (1) (a) (d) (e)	Sistem informasi , untuk otentikasi berbasis kata sandi: a. Menegakkan kompleksitas kata sandi minimum [Penugasan: persyaratan yang ditentukan organisasi untuk sensitivitas huruf besar, jumlah karakter, campuran huruf besar, huruf kecil, angka, dan karakter khusus, termasuk persyaratan minimum untuk setiap jenis]; d. Menegakkan batasan masa pakai minimum dan maksimum kata sandi [Penugasan: angka yang ditentukan organisasi untuk minimum seumur hidup, maksimum seumur hidup]; e. Melarang penggunaan kembali kata sandi untuk generasi [Penugasan: nomor yang ditentukan organisasi].	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan Centers for Internet Security (CIS) AWS Foundations Benchmark untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar),

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
			RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
IA-5 (4)	Organisasi menggunakan alat otomatis untuk menentukan apakah autentikator kata sandi cukup kuat untuk memenuhi [Penugasan: persyaratan yang ditentukan organisasi].	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan Centers for Internet Security (CIS) AWS Foundations Benchmark untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar),

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
			RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
IA-5 (7)	Organisasi memastikan bahwa autentikator statis yang tidak terenkripsi tidak disematkan dalam aplikasi atau skrip akses atau disimpan pada tombol fungsi.	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild. Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
IR-4 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung proses penanganan insiden.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
IR-4 (1)	Organisasi menggunakan mekanisme otomatis untuk mendukung proses penanganan insiden.	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
IR-6 (1)	Organisasi menggunakan mekanisme otomatis untuk membantu pelaporan insiden keamanan.	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
IR-7 (1)	Organisasi ini menggunakan mekanisme otomatis untuk meningkat kan ketersediaan informasi dan dukungan terkait respons insiden.	guardduty-non-arch ived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasark an tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunak an klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSe v (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratk an oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
RA-5	Organisasi: a. Memindai kerentana n dalam sistem informasi dan aplikasi yang dihosting [Penugasan: frekuensi yang ditentukan organisasi diidentif ikasi dan dilaporka n; and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/application s b. Menggunak an alat dan teknik pemindaian kerentana n yang memfasilitasi interoperabilitas antar alat dan mengotoma tiskan bagian dari proses manajemen kerentanan dengan menggunakan standar untuk: 1. Mencacah platform, kelemahan perangkat lunak, dan konfigurasi yang tidak tepat; 2. Memformat daftar periksa dan prosedur pengujian ; dan 3. Mengukur	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
	dampak kerentana n; c. Menganalisis laporan pemindaia n kerentanan dan hasil dari penilaian kontrol keamanan; d. Memulihkan kerentanan yang sah [Penugasa n: waktu respons yang ditentukan organisasi], sesuai dengan penilaian risiko organisasi; dan e. Membagika n informasi yang diperoleh dari proses pemindaian kerentana n dan penilaian kontrol keamanan dengan [Penugasa n: personel atau peran yang ditentuka n organisasi] untuk membantu menghilan gkan kerentanan serupa dalam sistem informasi lain (yaitu, kelemahan atau kekurangan sistemik).		

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
RA-5	Organisasi: a. Memindai kerentana n dalam sistem informasi dan aplikasi yang dihosting [Penugasan: frekuensi yang ditentukan organisasi diidentif ikasi dan dilaporka n; and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/application s b. Menggunak an alat dan teknik pemindaian kerentana n yang memfasilitasi interoperabilitas antar alat dan mengotoma tiskan bagian dari proses manajemen kerentanan dengan menggunakan standar untuk: 1. Mencacah platform, kelemahan perangkat lunak, dan konfigurasi yang tidak tepat; 2. Memformat daftar periksa dan prosedur pengujian ; dan 3. Mengukur	guardduty-non-arch ived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasark an tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunak an klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSe v (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratk an oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
	dampak kerentana n; c. Menganalisis laporan pemindaia n kerentanan dan hasil dari penilaian kontrol keamanan; d. Memulihkan kerentanan yang sah [Penugasa n: waktu respons yang ditentukan organisasi], sesuai dengan penilaian risiko organisasi; dan e. Membagika n informasi yang diperoleh dari proses pemindaian kerentana n dan penilaian kontrol keamanan dengan [Penugasa n: personel atau peran yang ditentuka n organisasi] untuk membantu menghilan gkan kerentanan serupa dalam sistem informasi lain (yaitu, kelemahan atau kekurangan sistemik).		

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SA-3 (a)	Organisasi: a. Mengelola sistem informasi menggunakan [Penugasan: siklus hidup pengembangan sistem yang ditentukan organisasi] yang menggabungkan pertimbangan keamanan informasi.	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild . Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SA-3 (a)	Organisasi: a. Mengelola sistem informasi menggunakan [Penugasan: siklus hidup pengembangan sistem yang ditentukan organisasi] yang menggabungkan pertimbangan keamanan informasi.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SA-3 (a)	Organisasi: a. Mengelola sistem informasi menggunakan [Penugasan: siklus hidup pengembangan sistem yang ditentukan organisasi] yang menggabungkan pertimbangan keamanan informasi.	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredenal masuk dalam lingkungan proyek Codebuild . AWS Gunakan OAuth alih-alih token akses pribadi atau kredensi masuk untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SA-10	Organisasi membutuhkan pengembang sistem informasi, komponen sistem, atau layanan sistem informasi untuk: a. Melakukan manajemen konfigura si selama sistem, komponen, atau layanan [Seleksi (satu atau lebih): desain; pengemban gan; implement asi; operasi]; b. Mendokume ntasikan, mengelola , dan mengontrol integritas perubahan pada [Penugasa n: item konfigura si yang ditentukan organisasi di bawah manajemen konfigura si]; c. Menerapkan hanya perubahan yang disetujui organisasi pada sistem, komponen, atau layanan; d. Mendokumentasikan perubahan yang disetujui pada sistem, komponen, atau	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
	layanan dan potensi dampak keamanan dari perubahan tersebut; dan e. Lacak kelemahan keamanan dan resolusi cacat dalam sistem, komponen, atau layanan dan laporkan temuan ke [Penugasan: personel yang ditentukan organisasi].		

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SA-10	Organisasi membutuhkan pengembang sistem informasi, komponen sistem, atau layanan sistem informasi untuk: a. Melakukan manajemen konfigurasi selama sistem, komponen, atau layanan [Seleksi (satu atau lebih): desain; pengembangan; implementasi; operasi]; b. Mendokumentasikan, mengelola, dan mengontrol integritas perubahan pada [Penugasan: item konfigurasi yang ditentukan organisasi di bawah manajemen konfigurasi]; c. Menerapkan hanya perubahan yang disetujui organisasi pada sistem, komponen, atau layanan; d. Mendokumentasikan perubahan yang disetujui pada sistem, komponen, atau	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan: rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
	layanan dan potensi dampak keamanan dari perubahan tersebut; dan e. Lacak kelemahan keamanan dan resolusi cacat dalam sistem, komponen, atau layanan dan laporkan temuan ke [Penugasan: personel yang ditentukan organisasi].		

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SA-10	Organisasi membutuhkan pengembang sistem informasi, komponen sistem, atau layanan sistem informasi untuk: a. Melakukan manajemen konfigura si selama sistem, komponen, atau layanan [Seleksi (satu atau lebih): desain; pengemban gan; implement asi; operasi]; b. Mendokume ntasikan, mengelola , dan mengontrol integritas perubahan pada [Penugasa n: item konfigura si yang ditentukan organisasi di bawah manajemen konfigura si]; c. Menerapkan hanya perubahan yang disetujui organisasi pada sistem, komponen, atau layanan; d. Mendokumentasikan perubahan yang disetujui pada sistem, komponen, atau	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
	layanan dan potensi dampak keamanan dari perubahan tersebut; dan e. Lacak kelemahan keamanan dan resolusi cacat dalam sistem, komponen, atau layanan dan laporkan temuan ke [Penugasan: personel yang ditentukan organisasi].		

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SA-10	Organisasi membutuhkan pengembang sistem informasi, komponen sistem, atau layanan sistem informasi untuk: a. Melakukan manajemen konfigura si selama sistem, komponen, atau layanan [Seleksi (satu atau lebih): desain; pengemban gan; implement asi; operasi]; b. Mendokume ntasikan, mengelola , dan mengontrol integritas perubahan pada [Penugasa n: item konfigura si yang ditentukan organisasi di bawah manajemen konfigura si]; c. Menerapkan hanya perubahan yang disetujui organisasi pada sistem, komponen, atau layanan; d. Mendokumentasikan perubahan yang disetujui pada sistem, komponen, atau	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
	layanan dan potensi dampak keamanan dari perubahan tersebut; dan e. Lacak kelemahan keamanan dan resolusi cacat dalam sistem, komponen, atau layanan dan laporkan temuan ke [Penugasan: personel yang ditentukan organisasi].		

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-2	Sistem informasi memisahkan fungsionalitas pengguna (termasuk layanan antarmuka pengguna) dari fungsi manajemen sistem informasi.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-2	Sistem informasi memisahkan fungsionalitas pengguna (termasuk layanan antarmuka pengguna) dari fungsi manajemen sistem informasi.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-4	Sistem informasi mencegah transfer informasi yang tidak sah dan tidak diinginkan dari sumber daya sistem bersama.	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	rds-cluster-multi-az-diaktifkan	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-5	Sistem informasi melindungi terhadap atau membatasi efek dari jenis serangan penolakan layanan berikut: [Penugasan: jenis serangan penolakan layanan yang ditentukan organisasi atau referensi ke sumber untuk informasi tersebut] dengan menggunakan [Penugasan: perlindungan keamanan yang ditentukan organisasi].	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigurasi ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapka n subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindun gan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi pada batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	s3- -blok account-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	alb-http-drop-invalid-Header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7	Sistem informasi: a. Memantau dan mengendalikan komunikasi di batas eksternal sistem dan pada batas-batas internal utama dalam sistem; b. Menerapkan subjaringan untuk komponen sistem yang dapat diakses publik yang [Seleksi: secara fisik; logis] terpisah dari jaringan organisasi internal; dan c. Terhubung ke jaringan eksternal atau sistem informasi hanya melalui antarmuka terkelola yang terdiri dari perangkat perlindungan batas yang diatur sesuai dengan arsitektur keamanan organisasi.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	s3- -blok account-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-7 (3)	Organisasi membatasi jumlah koneksi jaringan eksternal ke sistem informasi.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-8	Sistem informasi melindungi [Seleksi (satu atau lebih): kerahasiaan; integrita s] informasi yang dikirimkan.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-8	Sistem informasi melindungi [Seleksi (satu atau lebih): kerahasiaan; integrita s] informasi yang dikirimkan.	alb-http-drop-invalid-Header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-8	Sistem informasi melindungi [Seleksi (satu atau lebih): kerahasiaan; integrita s] informasi yang dikirimkan.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-n ode enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkrip si memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-8	Sistem informasi melindungi [Seleksi (satu atau lebih): kerahasiaan; integrita s] informasi yang dikirimkan.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-8	Sistem informasi melindungi [Seleksi (satu atau lebih): kerahasiaan; integrita s] informasi yang dikirimkan.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-8	Sistem informasi melindungi [Seleksi (satu atau lebih): kerahasiaan; integrita s] informasi yang dikirimkan.	s3- bucket-ssl-request s-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-8	Sistem informasi melindungi [Seleksi (satu atau lebih): kerahasiaan; integrita s] informasi yang dikirimkan.	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
SC-8 (1)	Sistem informasi menerapkan mekanisme kriptogra fi untuk [Seleksi (satu atau lebih): mencegah pengungka pan informasi yang tidak sah; mendeteks i perubahan informasi] selama transmisi kecuali dilindung i oleh [Penugasa n: perlindungan fisik alternatif yang ditentukan organisas i].	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-8 (1)	Sistem informasi menerapkan mekanisme kriptografi untuk [Seleksi (satu atau lebih): mencegah pengungkapan informasi yang tidak sah; mendeteksi perubahan informasi] selama transmisi kecuali dilindungi oleh [Penugasan: perlindungan fisik alternatif yang ditentukan organisasi].	alb-http-drop-invalid-Header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-8 (1)	Sistem informasi menerapkan mekanisme kriptografi untuk [Seleksi (satu atau lebih): mencegah pengungkapan informasi yang tidak sah; mendeteksi perubahan informasi] selama transmisi kecuali dilindungi oleh [Penugasan: perlindungan fisik alternatif yang ditentukan organisasi].	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-8 (1)	Sistem informasi menerapkan mekanisme kriptografi untuk [Seleksi (satu atau lebih): mencegah pengungkapan informasi yang tidak sah; mendeteksi perubahan informasi] selama transmisi kecuali dilindungi oleh [Penugasan: perlindungan fisik alternatif yang ditentukan organisasi].	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-8 (1)	Sistem informasi menerapkan mekanisme kriptografi untuk [Seleksi (satu atau lebih): mencegah pengungkapan informasi yang tidak sah; mendeteksi perubahan informasi] selama transmisi kecuali dilindungi oleh [Penugasan: perlindungan fisik alternatif yang ditentukan organisasi].	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-8 (1)	Sistem informasi menerapkan mekanisme kriptografi untuk [Seleksi (satu atau lebih): mencegah pengungkapan informasi yang tidak sah; mendeteksi perubahan informasi] selama transmisi kecuali dilindungi oleh [Penugasan: perlindungan fisik alternatif yang ditentukan organisasi].	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-8 (1)	Sistem informasi menerapkan mekanisme kriptografi untuk [Seleksi (satu atau lebih): mencegah pengungkapan informasi yang tidak sah; mendeteksi perubahan informasi] selama transmisi kecuali dilindungi oleh [Penugasan: perlindungan fisik alternatif yang ditentukan organisasi].	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
SC-12	Organisasi menetapkan dan mengelola kunci kriptografi untuk kriptografi yang diperlukan yang digunakan dalam sistem informasi sesuai dengan [Penugasan: persyaratan yang ditentukan organisasi untuk pembuatan kunci, distribusi, penyimpanan, akses, dan penghancuran].	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-12	Organisasi menetapkan dan mengelola kunci kriptografi untuk kriptografi yang diperlukan yang digunakan dalam sistem informasi sesuai dengan [Penugasan: persyaratan yang ditentukan organisasi untuk pembuatan kunci, distribusi, penyimpanan, akses, dan penghancuran].	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-12	Organisasi menetapkan dan mengelola kunci kriptografi untuk kriptografi yang diperlukan yang digunakan dalam sistem informasi sesuai dengan [Penugasan: persyaratan yang ditentukan organisasi untuk pembuatan kunci, distribusi, penyimpanan, akses, dan penghancuran].	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-13	Sistem informasi mengimplementasikan [Penugasan: penggunaan kriptografi yang ditentukan organisasi dan jenis kriptografi yang diperlukan untuk setiap penggunaan] sesuai dengan hukum federal yang berlaku, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar.	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
SC-13	Sistem informasi mengimplementasikan [Penugasan: penggunaan kriptografi yang ditentukan organisasi dan jenis kriptografi yang diperlukan untuk setiap penggunaan] sesuai dengan hukum federal yang berlaku, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-13	Sistem informasi mengimplementasikan [Penugasan: penggunaan kriptografi yang ditentukan organisasi dan jenis kriptografi yang diperlukan untuk setiap penggunaan] sesuai dengan hukum federal yang berlaku, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar.	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-13	Sistem informasi mengimplementasikan [Penugasan: penggunaan kriptografi yang ditentukan organisasi dan jenis kriptografi yang diperlukan untuk setiap penggunaan] sesuai dengan hukum federal yang berlaku, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-13	Sistem informasi mengimplementasikan [Penugasan: penggunaan kriptografi yang ditentukan organisasi dan jenis kriptografi yang diperlukan untuk setiap penggunaan] sesuai dengan hukum federal yang berlaku, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar.	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
SC-13	Sistem informasi mengimplementasikan [Penugasan: penggunaan kriptografi yang ditentukan organisasi dan jenis kriptografi yang diperlukan untuk setiap penggunaan] sesuai dengan hukum federal yang berlaku, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-13	Sistem informasi mengimplementasikan [Penugasan: penggunaan kriptografi yang ditentukan organisasi dan jenis kriptografi yang diperlukan untuk setiap penggunaan] sesuai dengan hukum federal yang berlaku, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar.	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
SC-13	Sistem informasi mengimplementasikan [Penugasan: penggunaan kriptografi yang ditentukan organisasi dan jenis kriptografi yang diperlukan untuk setiap penggunaan] sesuai dengan hukum federal yang berlaku, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-13	Sistem informasi mengimplementasikan [Penugasan: penggunaan kriptografi yang ditentukan organisasi dan jenis kriptografi yang diperlukan untuk setiap penggunaan] sesuai dengan hukum federal yang berlaku, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-13	Sistem informasi mengimplementasikan [Penugasan: penggunaan kriptografi yang ditentukan organisasi dan jenis kriptografi yang diperlukan untuk setiap penggunaan] sesuai dengan hukum federal yang berlaku, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-13	Sistem informasi mengimplementasikan [Penugasan: penggunaan kriptografi yang ditentukan organisasi dan jenis kriptografi yang diperlukan untuk setiap penggunaan] sesuai dengan hukum federal yang berlaku, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-13	Sistem informasi mengimplementasikan [Penugasan: penggunaan kriptografi yang ditentukan organisasi dan jenis kriptografi yang diperlukan untuk setiap penggunaan] sesuai dengan hukum federal yang berlaku, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-13	Sistem informasi mengimplementasikan [Penugasan: penggunaan kriptografi yang ditentukan organisasi dan jenis kriptografi yang diperlukan untuk setiap penggunaan] sesuai dengan hukum federal yang berlaku, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-13	Sistem informasi mengimplementasikan [Penugasan: penggunaan kriptografi yang ditentukan organisasi dan jenis kriptografi yang diperlukan untuk setiap penggunaan] sesuai dengan hukum federal yang berlaku, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar.	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-13	Sistem informasi mengimplementasikan [Penugasan: penggunaan kriptografi yang ditentukan organisasi dan jenis kriptografi yang diperlukan untuk setiap penggunaan] sesuai dengan hukum federal yang berlaku, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar.	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-13	Sistem informasi mengimplementasikan [Penugasan: penggunaan kriptografi yang ditentukan organisasi dan jenis kriptografi yang diperlukan untuk setiap penggunaan] sesuai dengan hukum federal yang berlaku, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar.	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-13	Sistem informasi mengimplementasikan kriptografi yang divalidasi FIPS atau disetujui NSA sesuai dengan hukum federal, Perintah Eksekutif, arahan, kebijakan, peraturan, dan standar yang berlaku.	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-23	Sistem informasi melindungi keaslian sesi komunikasi.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-23	Sistem informasi melindungi keaslian sesi komunikasi.	alb-http-drop-invalid-Header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-23	Sistem informasi melindungi keaslian sesi komunikasi.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-28	Sistem informasi melindungi [Seleksi (satu atau lebih): kerahasiaan; integritas] dari [Penugasan: informasi yang ditentukan organisasi saat istirahat].	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-28	Sistem informasi melindungi [Seleksi (satu atau lebih): kerahasiaan; integritas] dari [Penugasan: informasi yang ditentukan organisasi saat istirahat].	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-28	Sistem informasi melindungi [Seleksi (satu atau lebih): kerahasiaan; integrita s] dari [Penugasa n: informasi yang ditentukan organisasi saat istirahat].	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
SC-28	Sistem informasi melindungi [Seleksi (satu atau lebih): kerahasiaan; integrita s] dari [Penugasa n: informasi yang ditentukan organisasi saat istirahat].	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
SC-28	Sistem informasi melindungi [Seleksi (satu atau lebih): kerahasiaan; integrita s] dari [Penugasa n: informasi yang ditentukan organisasi saat istirahat].	elasticsearch-encr ypted-at-rest	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk domain OpenSearc h Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-28	Sistem informasi melindungi [Seleksi (satu atau lebih): kerahasiaan; integritas] dari [Penugasan: informasi yang ditentukan organisasi saat istirahat].	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
SC-28	Sistem informasi melindungi [Seleksi (satu atau lebih): kerahasiaan; integritas] dari [Penugasan: informasi yang ditentukan organisasi saat istirahat].	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-28	Sistem informasi melindungi [Seleksi (satu atau lebih): kerahasiaan; integritas] dari [Penugasan: informasi yang ditentukan organisasi saat istirahat].	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-28	Sistem informasi melindungi [Seleksi (satu atau lebih): kerahasiaan; integrita s] dari [Penugasa n: informasi yang ditentukan organisasi saat istirahat].	s3- bucket-default-loc k-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.
SC-28	Sistem informasi melindungi [Seleksi (satu atau lebih): kerahasiaan; integrita s] dari [Penugasa n: informasi yang ditentukan organisasi saat istirahat].	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-28	Sistem informasi melindungi [Seleksi (satu atau lebih): kerahasiaan; integrita s] dari [Penugasa n: informasi yang ditentukan organisasi saat istirahat].	sagemaker-endpoint -configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-28	Sistem informasi melindungi [Seleksi (satu atau lebih): kerahasiaan; integrita s] dari [Penugasa n: informasi yang ditentukan organisasi saat istirahat].	sagemaker-notebook -instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-28	Sistem informasi melindungi [Seleksi (satu atau lebih): kerahasiaan; integrita s] dari [Penugasa n: informasi yang ditentukan organisasi saat istirahat].	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-28	Sistem informasi melindungi [Seleksi (satu atau lebih): kerahasiaan; integrita s] dari [Penugasa n: informasi yang ditentukan organisasi saat istirahat].	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-28	Sistem informasi melindungi [Seleksi (satu atau lebih): kerahasiaan; integritas] dari [Penugasan: informasi yang ditentukan organisasi saat istirahat].	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-28	Sistem informasi melindungi [Seleksi (satu atau lebih): kerahasiaan; integritas] dari [Penugasan: informasi yang ditentukan organisasi saat istirahat].	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-36	Organisasi mendistribusikan [Penugasan: pemrosesan dan penyimpanan yang ditentukan organisasi] di beberapa lokasi fisik.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-36	Organisasi mendistribusikan [Penugasan: pemrosesan dan penyimpanan yang ditentukan organisasi] di beberapa lokasi fisik.	rds-cluster-multi-az-diaktifkan	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SC-36	Organisasi mendistribusikan [Penugasan: pemrosesan dan penyimpanan yang ditentukan organisasi] di beberapa lokasi fisik.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-2 (2)	Organisasi menggunakan mekanisme otomatis [Penugasan: frekuensi yang ditentukan organisasi] untuk menentukan keadaan komponen sistem informasi sehubungan dengan remediasi cacat.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-2 (2)	Organisasi menggunakan mekanisme otomatis [Penugasan: frekuensi yang ditentukan organisasi] untuk menentukan keadaan komponen sistem informasi sehubungan dengan remediasi cacat.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-2 (2)	Organisasi menggunakan mekanisme otomatis [Penugasan: frekuensi yang ditentukan organisasi] untuk menentukan keadaan komponen sistem informasi sehubungan dengan remediasi cacat.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-4 (1)	Organisasi menghubungkan dan mengonfigurasi alat deteksi intrusi individu ke dalam sistem deteksi intrusi di seluruh sistem informasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-4 (2)	Organisasi ini menggunakan alat otomatis untuk mendukung analisis peristiwa yang hampir real-time.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-4 (2)	Organisasi ini menggunakan alat otomatis untuk mendukung analisis peristiwa yang hampir real-time.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-4 (2)	Organisasi ini menggunakan alat otomatis untuk mendukung analisis peristiwa yang hampir real-time.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-4 (2)	Organisasi ini menggunakan alat otomatis untuk mendukung analisis peristiwa yang hampir real-time.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
SI-4 (2)	Organisasi ini menggunakan alat otomatis untuk mendukung analisis peristiwa yang hampir real-time.	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-4 (4)	Sistem informasi memantau lalu lintas komunikasi masuk dan keluar [Penugasan: frekuensi yang ditentukan organisasi] untuk aktivitas atau kondisi yang tidak biasa atau tidak sah.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-4 (4)	Sistem informasi memantau lalu lintas komunikasi masuk dan keluar [Penugasan: frekuensi yang ditentukan organisasi] untuk aktivitas atau kondisi yang tidak biasa atau tidak sah.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-4 (4)	Sistem informasi memantau lalu lintas komunikasi masuk dan keluar [Penugasan: frekuensi yang ditentukan organisasi] untuk aktivitas atau kondisi yang tidak biasa atau tidak sah.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-4 (4)	Sistem informasi memantau lalu lintas komunikasi masuk dan keluar [Penugasan: frekuensi yang ditentukan organisasi] untuk aktivitas atau kondisi yang tidak biasa atau tidak sah.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
SI-4 (5)	Sistem informasi memperingatkan [Penugasan: personel atau peran yang ditentukan organisasi] ketika indikasi kompromi atau potensi kompromi berikut terjadi: [Penugasan: indikator kompromi yang ditentukan organisasi].	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-4 (5)	Sistem informasi memperingatkan [Penugasan: personel atau peran yang ditentukan organisasi] ketika indikasi kompromi atau potensi kompromi berikut terjadi: [Penugasan: indikator kompromi yang ditentukan organisasi].	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-4 (5)	Sistem informasi memperingatkan [Penugasan: personel atau peran yang ditentukan organisasi] ketika indikasi kompromi atau potensi kompromi berikut terjadi: [Penugasan: indikator kompromi yang ditentukan organisasi].	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-4 (5)	Sistem informasi memperingatkan [Penugasan: personel atau peran yang ditentukan organisasi] ketika indikasi kompromi atau potensi kompromi berikut terjadi: [Penugasan: indikator kompromi yang ditentukan organisasi].	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
SI-4 (16)	Organisasi menghubungkan informasi dari alat pemantauan yang digunakan di seluruh sistem informasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-4 (16)	Organisasi menghubungkan informasi dari alat pemantauan yang digunakan di seluruh sistem informasi.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-4 (a) (b) (c)	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1. Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2. Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c. Menyebarkan perangkat pemantauan: i. secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan (ii) di lokasi ad hoc dalam sistem untuk melacak jenis transaksi	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
	tertentu yang menarik bagi organisasi.		

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-4 (a) (b) (c)	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1. Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2. Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c. Menyebarkan perangkat pemantauan: i. secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan (ii) di lokasi ad hoc dalam sistem untuk melacak jenis transaksi	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan: rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
	tertentu yang menarik bagi organisasi.		

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-4 (a) (b) (c)	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1. Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2. Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c. Menyebarkan perangkat pemantauan: i. secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan (ii) di lokasi ad hoc dalam sistem untuk melacak jenis transaksi	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
	tertentu yang menarik bagi organisasi.		

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-4 (a) (b) (c)	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1. Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2. Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c. Menyebarkan perangkat pemantauan: i. secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan (ii) di lokasi ad hoc dalam sistem untuk melacak jenis transaksi	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
	tertentu yang menarik bagi organisasi.		

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-4 (a) (b) (c)	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1. Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2. Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c. Menyebarkan perangkat pemantauan: i. secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan (ii) di lokasi ad hoc dalam sistem untuk melacak jenis transaksi	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
	tertentu yang menarik bagi organisasi.		

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-4 (a) (b) (c)	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1. Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2. Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c. Menyebarkan perangkat pemantauan: i. secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan (ii) di lokasi ad hoc dalam sistem untuk melacak jenis transaksi	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai sebenarnya harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
	tertentu yang menarik bagi organisasi.		

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-4 (a) (b) (c)	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1. Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2. Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c. Menyebarkan perangkat pemantauan: i. secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan (ii) di lokasi ad hoc dalam sistem untuk melacak jenis transaksi	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
	tertentu yang menarik bagi organisasi.		

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-4 (a) (b) (c)	Organisasi: a. Memantau sistem informasi untuk mendeteksi: 1. Serangan dan indikator serangan potensial sesuai dengan [Penugasan: tujuan pemantauan yang ditentukan organisasi]; dan 2. Koneksi lokal, jaringan, dan jarak jauh yang tidak sah; b. Mengidentifikasi penggunaan sistem informasi yang tidak sah melalui [Penugasan: teknik dan metode yang ditentukan organisasi]; c. Menyebarkan perangkat pemantauan: i. secara strategis dalam sistem informasi untuk mengumpulkan informasi penting yang ditentukan organisasi; dan (ii) di lokasi ad hoc dalam sistem untuk melacak jenis transaksi	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
	tertentu yang menarik bagi organisasi.		
SI-7	Organisasi menggunakan alat verifikasi integritas untuk mendeteksi perubahan yang tidak sah pada [Penugasan: perangkat lunak, firmware, dan informasi yang ditentukan organisasi].	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-7 (1)	Sistem informasi melakukan pemeriksaan integritas [Penugasan: perangkat lunak, firmware, dan informasi yang ditentukan organisasi] [Seleksi (satu atau lebih): saat startup; di [Penugasan: keadaan transisi yang ditentukan organisasi atau peristiwa yang relevan dengan keamanan]; [Penugasan: frekuensi yang ditentukan organisasi]].	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-7 (1)	Sistem informasi melakukan pemeriksaan integritas [Penugasan: perangkat lunak, firmware, dan informasi yang ditentukan organisasi] [Seleksi (satu atau lebih): saat startup; di [Penugasan: keadaan transisi yang ditentukan organisasi atau peristiwa yang relevan dengan keamanan]; [Penugasan: frekuensi yang ditentukan organisasi]].	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-7 (1)	Sistem informasi melakukan pemeriksaan integritas [Penugasan: perangkat lunak, firmware, dan informasi yang ditentukan organisasi] [Seleksi (satu atau lebih): saat startup; di [Penugasan: keadaan transisi yang ditentukan organisasi atau peristiwa yang relevan dengan keamanan]; [Penugasan: frekuensi yang ditentukan organisasi]].	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan cadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	efs-in-backup-plan	Untuk membantu proses pencadang an data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	dynamodb-in-backup-plan	Untuk membantu proses pencadang an data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Config Aturan	Bimbingan
SI-12	Organisasi menangani dan menyimpan informasi dalam sistem informasi dan output informasi dari sistem sesuai dengan hukum federal yang berlaku, Perintah Eksekutif , arahan, kebijakan , peraturan, standar, dan persyaratan operasional.	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk NIST 800-53 rev 4.

Praktik Terbaik Operasional untuk NIST 800-53 rev 5

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini menyediakan contoh pemetaan antara aturan NIST 800-53 dan Config terkelola AWS . Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan berhubungan dengan satu atau beberapa kontrol NIST 800-53. Kontrol NIST 800-53 dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (4)	Manajemen Akun | Tindakan Audit Otomatis	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.
AC-2 (4)	Manajemen Akun | Tindakan Audit Otomatis	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.
AC-2 (4)	Manajemen Akun | Tindakan Audit Otomatis	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (4)	Manajemen Akun | Tindakan Audit Otomatis	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
AC-2 (4)	Manajemen Akun | Tindakan Audit Otomatis	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (4)	Manajemen Akun | Tindakan Audit Otomatis	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
AC-2 (4)	Manajemen Akun | Tindakan Audit Otomatis	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (4)	Manajemen Akun | Tindakan Audit Otomatis	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (4)	Manajemen Akun | Tindakan Audit Otomatis	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2 (12)	Manajemen Akun | Pemantauan Akun untuk Penggunaan Atipikal	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	Pengelolaan Akun	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	Pengelolaan Akun	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	Pengelolaan Akun	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	Pengelolaan Akun	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
AC-2	Pengelolaan Akun	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	Pengelolaan Akun	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-2	Pengelolaan Akun	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3 (15)	Penegakan Akses | Kontrol Akses Diskresioner dan Wajib	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.
AC-3 (15)	Penegakan Akses | Kontrol Akses Diskresioner dan Wajib	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3 (15)	Penegakan Akses | Kontrol Akses Diskresioner dan Wajib	ecs-containers-readonly-access	Mengaktifkan akses baca saja ke wadah Amazon Elastic Container Service (ECS) dapat membantu mematuhi prinsip hak istimewa yang paling rendah. Opsi ini dapat mengurangi vektor serangan karena sistem file instance container tidak dapat dimodifikasi kecuali jika memiliki izin baca-tulis eksplisit.
AC-3 (15)	Penegakan Akses | Kontrol Akses Diskresioner dan Wajib	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3 (15)	Penegakan Akses | Kontrol Akses Diskresioner dan Wajib	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3 (15)	Penegakan Akses | Kontrol Akses Diskresioner dan Wajib	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3 (15)	Penegakan Akses | Kontrol Akses Diskresioner dan Wajib	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3 (15)	Penegakan Akses | Kontrol Akses Diskresioner dan Wajib	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3 (15)	Penegakan Akses | Kontrol Akses Diskresioner dan Wajib	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3 (15)	Penegakan Akses | Kontrol Akses Diskresioner dan Wajib	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3 (15)	Penegakan Akses | Kontrol Akses Diskresioner dan Wajib	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3 (15)	Penegakan Akses | Kontrol Akses Diskresioner dan Wajib	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3 (15)	Penegakan Akses | Kontrol Akses Diskresioner dan Wajib	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3 (15)	Penegakan Akses | Kontrol Akses Diskresioner dan Wajib	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3 (15)	Penegakan Akses | Kontrol Akses Diskresioner dan Wajib	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3 (15)	Penegakan Akses | Kontrol Akses Diskresioner dan Wajib	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3 (15)	Penegakan Akses | Kontrol Akses Diskresioner dan Wajib	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3 (15)	Penegakan Akses | Kontrol Akses Diskresioner dan Wajib	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
AC-3 (15)	Penegakan Akses | Kontrol Akses Diskresioner dan Wajib	secretsmanager-rotation-enabled-check	Aturan ini memastikan AWS rahasia Secrets Manager telah diaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Penegakan Akses	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Penegakan Akses	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.
AC-3	Penegakan Akses	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Penegakan Akses	ecs-containers-readonly-access	Mengaktifkan akses baca saja ke wadah Amazon Elastic Container Service (ECS) dapat membantu mematuhi prinsip hak istimewa yang paling rendah. Opsi ini dapat mengurangi vektor serangan karena sistem file instance container tidak dapat dimodifikasi kecuali jika memiliki izin baca-tulis eksplisit.
AC-3	Penegakan Akses	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Penegakan Akses	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Penegakan Akses	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
AC-3	Penegakan Akses	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Penegakan Akses	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-3	Penegakan Akses	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-3	Penegakan Akses	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Penegakan Akses	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
AC-3	Penegakan Akses	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Penegakan Akses	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Penegakan Akses	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
AC-3	Penegakan Akses	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Penegakan Akses	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Penegakan Akses	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Penegakan Akses	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Penegakan Akses	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Penegakan Akses	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Penegakan Akses	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
AC-3	Penegakan Akses	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Penegakan Akses	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Penegakan Akses	s3- account-level-publ ic-access -blok-per iodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Penegakan Akses	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
AC-3	Penegakan Akses	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Penegakan Akses	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
AC-3	Penegakan Akses	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-3	Penegakan Akses	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
AC-4 (26)	Penegakan Arus Informasi | Tindakan Penyaringan Audit	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4 (26)	Penegakan Arus Informasi | Tindakan Penyaringan Audit	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4 (26)	Penegakan Arus Informasi | Tindakan Penyaringan Audit	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4 (26)	Penegakan Arus Informasi | Tindakan Penyaringan Audit	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
AC-4 (26)	Penegakan Arus Informasi | Tindakan Penyaringan Audit	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4 (26)	Penegakan Arus Informasi | Tindakan Penyaringan Audit	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
AC-4 (26)	Penegakan Arus Informasi | Tindakan Penyaringan Audit	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4 (26)	Penegakan Arus Informasi | Tindakan Penyaringan Audit	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
AC-4 (26)	Penegakan Arus Informasi | Tindakan Penyaringan Audit	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4 (26)	Penegakan Arus Informasi | Tindakan Penyaringan Audit	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4 (26)	Penegakan Arus Informasi | Tindakan Penyaringan Audit	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDbEncrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4 (26)	Penegakan Arus Informasi | Tindakan Penyaringan Audit	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-4 (26)	Penegakan Arus Informasi | Tindakan Penyaringan Audit	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
AC-5	Pemisahan Tugas	ecs-containers-readonly-access	Mengaktifkan akses baca saja ke wadah Amazon Elastic Container Service (ECS) dapat membantu mematuhi prinsip hak istimewa yang paling rendah. Opsi ini dapat mengurangi vektor serangan karena sistem file instance container tidak dapat dimodifikasi kecuali jika memiliki izin baca-tulis eksplisit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-5	Pemisahan Tugas	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.
AC-5	Pemisahan Tugas	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-5	Pemisahan Tugas	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-5	Pemisahan Tugas	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
AC-5	Pemisahan Tugas	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (2)	Keistimewaan Terkecil | Akses Tanpa Hak Istimewa untuk Fungsi Nonkeamanan	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (2)	Keistimewaan Terkecil | Akses Tanpa Hak Istimewa untuk Fungsi Nonkeamanan	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (2)	Keistimewaan Terkecil | Akses Tanpa Hak Istimewa untuk Fungsi Nonkeamanan	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (3)	Hak Istimewa Terkecil | Akses Jaringan ke Perintah Istimewa	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (3)	Hak Istimewa Terkecil | Akses Jaringan ke Perintah Istimewa	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (3)	Hak Istimewa Terkecil | Akses Jaringan ke Perintah Istimewa	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (3)	Hak Istimewa Terkecil | Akses Jaringan ke Perintah Istimewa	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
AC-6 (3)	Hak Istimewa Terkecil | Akses Jaringan ke Perintah Istimewa	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (3)	Hak Istimewa Terkecil | Akses Jaringan ke Perintah Istimewa	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (9)	Hak Istimewa Terkecil | Log Penggunaan Fungsi Istimewa	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (9)	Hak Istimewa Terkecil | Log Penggunaan Fungsi Istimewa	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (9)	Hak Istimewa Terkecil | Log Penggunaan Fungsi Istimewa	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.
AC-6 (9)	Hak Istimewa Terkecil | Log Penggunaan Fungsi Istimewa	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (9)	Hak Istimewa Terkecil | Log Penggunaan Fungsi Istimewa	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
AC-6 (9)	Hak Istimewa Terkecil | Log Penggunaan Fungsi Istimewa	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (9)	Hak Istimewa Terkecil | Log Penggunaan Fungsi Istimewa	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (9)	Hak Istimewa Terkecil | Log Penggunaan Fungsi Istimewa	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (9)	Hak Istimewa Terkecil | Log Penggunaan Fungsi Istimewa	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (10)	Hak Istimewa Terkecil | Melarang Pengguna yang Tidak Berhak Istimewa Menjalankan Fungsi Istimewa	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (10)	Hak Istimewa Terkecil | Melarang Pengguna yang Tidak Berhak Istimewa Menjalankan Fungsi Istimewa	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-6 (10)	Hak Istimewa Terkecil | Melarang Pengguna yang Tidak Berhak Istimewa Menjalankan Fungsi Istimewa	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (2)	Akses Jarak Jauh | Perlindungan Kerahasiaan dan Integritas Menggunakan Enkripsi	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
AC-17 (2)	Akses Jarak Jauh | Perlindungan Kerahasiaan dan Integritas Menggunakan Enkripsi	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (2)	Akses Jarak Jauh | Perlindungan Kerahasiaan dan Integritas Menggunakan Enkripsi	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
AC-17 (2)	Akses Jarak Jauh | Perlindungan Kerahasiaan dan Integritas Menggunakan Enkripsi	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (2)	Akses Jarak Jauh | Perlindungan Kerahasiaan dan Integritas Menggunakan Enkripsi	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.
AC-17 (2)	Akses Jarak Jauh | Perlindungan Kerahasiaan dan Integritas Menggunakan Enkripsi	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-17 (2)	Akses Jarak Jauh | Perlindungan Kerahasiaan dan Integritas Menggunakan Enkripsi	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
AC-21	Berbagi Informasi	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21	Berbagi Informasi	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21	Berbagi Informasi	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
AC-21	Berbagi Informasi	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21	Berbagi Informasi	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
AC-21	Berbagi Informasi	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21	Berbagi Informasi	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
AC-21	Berbagi Informasi	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21	Berbagi Informasi	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21	Berbagi Informasi	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21	Berbagi Informasi	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21	Berbagi Informasi	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
AC-21	Berbagi Informasi	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21	Berbagi Informasi	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21	Berbagi Informasi	s3- account-level-publ ic-access -blok-per iodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21	Berbagi Informasi	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
AC-21	Berbagi Informasi	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21	Berbagi Informasi	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
AC-21	Berbagi Informasi	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AC-21	Berbagi Informasi	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
AU-2	Pencatatan Acara	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2	Pencatatan Acara	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2	Pencatatan Acara	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2	Pencatatan Acara	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2	Pencatatan Acara	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
AU-2	Pencatatan Acara	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2	Pencatatan Acara	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
AU-2	Pencatatan Acara	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2	Pencatatan Acara	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
AU-2	Pencatatan Acara	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2	Pencatatan Acara	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2	Pencatatan Acara	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-2	Pencatatan Acara	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
AU-3	Isi Catatan Audit	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	Isi Catatan Audit	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	Isi Catatan Audit	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	Isi Catatan Audit	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
AU-3	Isi Catatan Audit	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	Isi Catatan Audit	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
AU-3	Isi Catatan Audit	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	Isi Catatan Audit	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
AU-3	Isi Catatan Audit	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	Isi Catatan Audit	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	Isi Catatan Audit	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDbEncrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	Isi Catatan Audit	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-3	Isi Catatan Audit	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
AU-6 (1)	Tinjauan Rekaman Audit, Analisis, dan Pelaporan | Integrasi Proses Otomatis	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1)	Tinjauan Rekaman Audit, Analisis, dan Pelaporan | Integrasi Proses Otomatis	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1)	Tinjauan Rekaman Audit, Analisis, dan Pelaporan | Integrasi Proses Otomatis	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (1)	Tinjauan Rekaman Audit, Analisis, dan Pelaporan | Integrasi Proses Otomatis	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (3)	Tinjauan Rekaman Audit, Analisis, dan Pelaporan | Korelasikan Repositori Catatan Audit	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (3)	Tinjauan Rekaman Audit, Analisis, dan Pelaporan | Korelasikan Repositori Catatan Audit	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (3)	Tinjauan Rekaman Audit, Analisis, dan Pelaporan | Korelasikan Repositori Catatan Audit	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (3)	Tinjauan Rekaman Audit, Analisis, dan Pelaporan | Korelasikan Repositori Catatan Audit	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
AU-6 (3)	Tinjauan Rekaman Audit, Analisis, dan Pelaporan | Korelasikan Repositori Catatan Audit	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (3)	Tinjauan Rekaman Audit, Analisis, dan Pelaporan | Korelasi an Repositori Catatan Audit	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
AU-6 (3)	Tinjauan Rekaman Audit, Analisis, dan Pelaporan | Korelasi an Repositori Catatan Audit	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (3)	Tinjauan Rekaman Audit, Analisis, dan Pelaporan | Korelasikan Repositori Catatan Audit	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
AU-6 (3)	Tinjauan Rekaman Audit, Analisis, dan Pelaporan | Korelasikan Repositori Catatan Audit	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (3)	Tinjauan Rekaman Audit, Analisis, dan Pelaporan | Korelasik an Repositori Catatan Audit	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (3)	Tinjauan Rekaman Audit, Analisis, dan Pelaporan | Korelasikan Repositori Catatan Audit	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (3)	Tinjauan Rekaman Audit, Analisis, dan Pelaporan | Korelasikan Repositori Catatan Audit	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (3)	Tinjauan Rekaman Audit, Analisis, dan Pelaporan | Korelasikan Repositori Catatan Audit	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
AU-6 (4)	Tinjauan, Analisis, dan Pelaporan Catatan Audit | Tinjauan dan Analisis Pusat	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (4)	Tinjauan, Analisis, dan Pelaporan Catatan Audit | Tinjauan dan Analisis Pusat	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (4)	Tinjauan, Analisis, dan Pelaporan Catatan Audit | Tinjauan dan Analisis Pusat	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (4)	Tinjauan, Analisis, dan Pelaporan Catatan Audit | Tinjauan dan Analisis Pusat	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
AU-6 (4)	Tinjauan, Analisis, dan Pelaporan Catatan Audit | Tinjauan dan Analisis Pusat	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (4)	Tinjauan, Analisis, dan Pelaporan Catatan Audit | Tinjauan dan Analisis Pusat	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
AU-6 (4)	Tinjauan, Analisis, dan Pelaporan Catatan Audit | Tinjauan dan Analisis Pusat	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (4)	Tinjauan, Analisis, dan Pelaporan Catatan Audit | Tinjauan dan Analisis Pusat	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
AU-6 (4)	Tinjauan, Analisis, dan Pelaporan Catatan Audit | Tinjauan dan Analisis Pusat	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (4)	Tinjauan, Analisis, dan Pelaporan Catatan Audit | Tinjauan dan Analisis Pusat	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (4)	Tinjauan, Analisis, dan Pelaporan Catatan Audit | Tinjauan dan Analisis Pusat	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (4)	Tinjauan, Analisis, dan Pelaporan Catatan Audit | Tinjauan dan Analisis Pusat	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (4)	Tinjauan, Analisis, dan Pelaporan Catatan Audit | Tinjauan dan Analisis Pusat	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
AU-6 (5)	Peninjauan Rekaman Audit, Analisis, dan Pelaporan | Analisis Terpadu Rekaman Audit	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (5)	Peninjauan Rekaman Audit, Analisis, dan Pelaporan | Analisis Terpadu Rekaman Audit	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (5)	Peninjauan Rekaman Audit, Analisis, dan Pelaporan | Analisis Terpadu Rekaman Audit	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-6 (5)	Peninjauan Rekaman Audit, Analisis, dan Pelaporan | Analisis Terpadu Rekaman Audit	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-7 (1)	Pengurangan Rekaman Audit dan Pembuatan Laporan | Pemrosesan Otomatis	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
AU-9 (2)	Perlindungan Informasi Audit | Simpan pada Sistem atau Komponen Fisik Terpisah	s3- version-lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihkan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-9 (2)	Perlindungan Informasi Audit | Simpan pada Sistem atau Komponen Fisik Terpisah	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-9 (2)	Perlindungan Informasi Audit | Simpan pada Sistem atau Komponen Fisik Terpisah	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-9 (7)	Perlindungan Informasi Audit | Simpan pada Komponen dengan Sistem Operasi yang Berbeda	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
AU-9	Perlindungan Informasi Audit	s3- default-encryption -kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-9	Perlindungan Informasi Audit	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
AU-9	Perlindungan Informasi Audit	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrai l jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-9	Perlindungan Informasi Audit	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-9	Perlindungan Informasi Audit	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
AU-10	Non-penolakan	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-10	Non-penolakan	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-10	Non-penolakan	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-10	Non-penolakan	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-10	Non-penolakan	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
AU-10	Non-penolakan	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-10	Non-penolakan	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
AU-10	Non-penolakan	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-10	Non-penolakan	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
AU-10	Non-penolakan	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-10	Non-penolakan	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-10	Non-penolakan	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Pembuatan Rekaman Audit	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Pembuatan Rekaman Audit	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Pembuatan Rekaman Audit	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Pembuatan Rekaman Audit	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
AU-12	Pembuatan Rekaman Audit	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Pembuatan Rekaman Audit	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
AU-12	Pembuatan Rekaman Audit	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Pembuatan Rekaman Audit	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
AU-12	Pembuatan Rekaman Audit	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Pembuatan Rekaman Audit	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Pembuatan Rekaman Audit	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Pembuatan Rekaman Audit	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-12	Pembuatan Rekaman Audit	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
AU-14 (1)	Audit Sesi | Sistem Start-up	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7	Pemantauan Berkelanjutan	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.
CA-7	Pemantauan Berkelanjutan	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7	Pemantauan Berkelanjutan	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7	Pemantauan Berkelanjutan	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7	Pemantauan Berkelanjutan	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7	Pemantauan Berkelanjutan	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
CA-7	Pemantauan Berkelanjutan	s3- event-notifications-enabled	Pemberitahuan peristiwa Amazon S3 dapat memberi tahu personel terkait tentang modifikasi yang tidak disengaja atau disengaja pada objek bucket Anda. Contoh peringatan meliputi: objek baru adalah pembuatan, penghapusan objek, restorasi objek, objek yang hilang dan direplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7	Pemantauan Berkelanjutan	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7	Pemantauan Berkelanjutan	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
CA-7	Pemantauan Berkelanjutan	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7	Pemantauan Berkelanjutan	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7	Pemantauan Berkelanjutan	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7	Pemantauan Berkelanjutan	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
CA-7	Pemantauan Berkelanjutan	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7	Pemantauan Berkelanjutan	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7	Pemantauan Berkelanjutan	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7	Pemantauan Berkelanjutan	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
CA-7	Pemantauan Berkelanjutan	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7	Pemantauan Berkelanjutan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7	Pemantauan Berkelanjutan	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7	Pemantauan Berkelanjutan	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-7	Pemantauan Berkelanjutan	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
CA-9 (1)	Koneksi Sistem Internal | Pemeriksaan Kepatuhan	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-9 (1)	Koneksi Sistem Internal | Pemeriksa an Kepatuhan	codebuild-project-artifact-encryption	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk AWS CodeBuild artefak Anda.
CA-9 (1)	Koneksi Sistem Internal | Pemeriksa an Kepatuhan	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindung i data tersebut. Secara default, tabel DynamoDB dienkrips i dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-9 (1)	Koneksi Sistem Internal | Pemeriksa an Kepatuhan	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CA-9 (1)	Koneksi Sistem Internal | Pemeriksa an Kepatuhan	kinesis-stream-encrypted	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-9 (1)	Koneksi Sistem Internal | Pemeriksa an Kepatuhan	rds-instance-default-admin-periksa	Karena nama pengguna default adalah pengetahu an publik, mengubah nama pengguna default dapat membantu mengurangi permukaan serangan untuk instans database Amazon Relational Database Service (Amazon RDS) Anda.
CA-9 (1)	Koneksi Sistem Internal | Pemeriksa an Kepatuhan	rds-snapshot-encry pted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-9 (1)	Koneksi Sistem Internal | Pemeriksa an Kepatuhan	s3- default-encryption -kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CA-9 (1)	Koneksi Sistem Internal | Pemeriksa an Kepatuhan	sagemaker-notebook -instance-kms-kunci- dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-9 (1)	Koneksi Sistem Internal | Pemeriksaan Kepatuhan	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CA-9 (1)	Koneksi Sistem Internal | Pemeriksaan Kepatuhan	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-9 (1)	Koneksi Sistem Internal | Pemeriksa an Kepatuhan	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrai l jejak Anda.
CA-9 (1)	Koneksi Sistem Internal | Pemeriksa an Kepatuhan	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-9 (1)	Koneksi Sistem Internal | Pemeriksaan Kepatuhan	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-9 (1)	Koneksi Sistem Internal | Pemeriksa an Kepatuhan	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.
CA-9 (1)	Koneksi Sistem Internal | Pemeriksa an Kepatuhan	ec2- volume-inuse-check	Aturan ini memastika n bahwa volume Amazon Elastic Block Store yang dilampirk an ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentika n, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-9 (1)	Koneksi Sistem Internal | Pemeriksaan Kepatuhan	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
CA-9 (1)	Koneksi Sistem Internal | Pemeriksaan Kepatuhan	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-9 (1)	Koneksi Sistem Internal | Pemeriksaan Kepatuhan	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
CA-9 (1)	Koneksi Sistem Internal | Pemeriksaan Kepatuhan	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-9 (1)	Koneksi Sistem Internal | Pemeriksaan Kepatuhan	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
CA-9 (1)	Koneksi Sistem Internal | Pemeriksaan Kepatuhan	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-9 (1)	Koneksi Sistem Internal | Pemeriksaan Kepatuhan	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-9 (1)	Koneksi Sistem Internal | Pemeriksaan Kepatuhan	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-9 (1)	Koneksi Sistem Internal | Pemeriksaan Kepatuhan	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-9 (1)	Koneksi Sistem Internal | Pemeriksaan Kepatuhan	redshift-default-admin-check	Karena nama pengguna default adalah pengetahuan publik, mengubah nama pengguna default dapat membantu mengurangi permukaan serangan untuk klaster Amazon Redshift Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-9 (1)	Koneksi Sistem Internal | Pemeriksaan Kepatuhan	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-9 (1)	Koneksi Sistem Internal | Pemeriksa an Kepatuhan	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
CA-9 (1)	Koneksi Sistem Internal | Pemeriksa an Kepatuhan	sagemaker-endpoint -configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CA-9 (1)	Koneksi Sistem Internal | Pemeriksaan Kepatuhan	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2 (2)	Konfigurasi Dasar | Dukungan Otomasi untuk Akurasi dan Mata Uang	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2 (2)	Konfigurasi Dasar | Dukungan Otomasi untuk Akurasi dan Mata Uang	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2 (2)	Konfigurasi Dasar | Dukungan Otomasi untuk Akurasi dan Mata Uang	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.
CM-2 (2)	Konfigurasi Dasar | Dukungan Otomasi untuk Akurasi dan Mata Uang	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2 (2)	Konfigurasi Dasar | Dukungan Otomasi untuk Akurasi dan Mata Uang	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2 (2)	Konfigurasi Dasar | Dukungan Otomasi untuk Akurasi dan Mata Uang	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Konfigurasi Dasar	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.
CM-2	Konfigurasi Dasar	rds-instance-default-admin-periksa	Karena nama pengguna default adalah pengetahuan publik, mengubah nama pengguna default dapat membantu mengurangi permukaan serangan untuk instans database Amazon Relational Database Service (Amazon RDS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Konfigurasi Dasar	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Konfigurasi Dasar	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Konfigurasi Dasar	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.
CM-2	Konfigurasi Dasar	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Konfigurasi Dasar	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Konfigurasi Dasar	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Konfigurasi Dasar	redshift-default-admin-check	Karena nama pengguna default adalah pengetahuan publik, mengubah nama pengguna default dapat membantu mengurangi permukaan serangan untuk klaster Amazon Redshift Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-2	Konfigurasi Dasar	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-3 (6)	Kontrol Perubahan Konfigurasi | Manajemen Kriptografi	codebuild-project-artifact-encryption	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk AWS CodeBuild artefak Anda.
CM-3 (6)	Kontrol Perubahan Konfigurasi | Manajemen Kriptografi	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-3 (6)	Kontrol Perubahan Konfigurasi | Manajemen Kriptografi	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CM-3 (6)	Kontrol Perubahan Konfigurasi | Manajemen Kriptografi	kinesis-stream-encrypted	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-3 (6)	Kontrol Perubahan Konfigurasi | Manajemen Kriptografi	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CM-3 (6)	Kontrol Perubahan Konfigurasi | Manajemen Kriptografi	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-3 (6)	Kontrol Perubahan Konfigurasi | Manajemen Kriptografi	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-3 (6)	Kontrol Perubahan Konfigurasi | Manajemen Kriptografi	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CM-3 (6)	Kontrol Perubahan Konfigurasi | Manajemen Kriptografi	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-3 (6)	Kontrol Perubahan Konfigurasi | Manajemen Kriptografi	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
CM-3 (6)	Kontrol Perubahan Konfigurasi | Manajemen Kriptografi	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
CM-3 (6)	Kontrol Perubahan Konfigurasi | Manajemen Kriptografi	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-3 (6)	Kontrol Perubahan Konfigurasi | Manajemen Kriptografi	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
CM-3 (6)	Kontrol Perubahan Konfigurasi | Manajemen Kriptografi	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
CM-3 (6)	Kontrol Perubahan Konfigurasi | Manajemen Kriptografi	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-3 (6)	Kontrol Perubahan Konfigurasi | Manajemen Kriptografi	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-3 (6)	Kontrol Perubahan Konfigurasi | Manajemen Kriptografi	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CM-3 (6)	Kontrol Perubahan Konfigurasi | Manajemen Kriptografi	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-3 (6)	Kontrol Perubahan Konfigurasi | Manajemen Kriptografi	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
CM-3 (6)	Kontrol Perubahan Konfigurasi | Manajemen Kriptografi	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-3	Kontrol Perubahan Konfigurasi	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-3	Kontrol Perubahan Konfigurasi	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-7	Fungsionalitas Paling Sedikit	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.
CM-7	Fungsionalitas Paling Sedikit	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-7	Fungsionalitas Paling Sedikit	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-8 (1)	Inventaris Komponen Sistem | Pembaruan Selama Instalasi dan Penghapusan	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-8 (1)	Inventaris Komponen Sistem | Pembaruan Selama Instalasi dan Penghapusan	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-8 (2)	Inventaris Komponen Sistem | Pemeliharaan Otomatis	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-8 (3)	Inventaris Komponen Sistem | Deteksi Komponen Tidak Sah Otomatis	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-8 (3)	Inventaris Komponen Sistem | Deteksi Komponen Tidak Sah Otomatis	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-8 (3)	Inventaris Komponen Sistem | Deteksi Komponen Tidak Sah Otomatis	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-8 (3)	Inventaris Komponen Sistem | Deteksi Komponen Tidak Sah Otomatis	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-8	Inventaris Komponen Sistem	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CM-8	Inventaris Komponen Sistem	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi ke instans terkelola Anda dan memungkinkan Anda untuk menetapkan garis dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-2 (2)	Rencana Kontinjensi | Perencanaan Kapasitas	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-2 (2)	Rencana Kontinjensi | Perencanaan Kapasitas	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (1)	Situs Penyimpanan Alternatif | Pemisahan dari Situs Utama	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (1)	Situs Penyimpanan Alternatif | Pemisahan dari Situs Utama	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (1)	Situs Penyimpanan Alternatif | Pemisahan dari Situs Utama	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (1)	Situs Penyimpanan Alternatif | Pemisahan dari Situs Utama	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (1)	Situs Penyimpanan Alternatif | Pemisahan dari Situs Utama	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (1)	Situs Penyimpanan Alternatif | Pemisahan dari Situs Utama	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (1)	Situs Penyimpanan Alternatif | Pemisahan dari Situs Utama	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (1)	Situs Penyimpanan Alternatif | Pemisahan dari Situs Utama	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (2)	Situs Penyimpan an Alternatif | Waktu Pemulihan dan Tujuan Titik Pemulihan	dynamodb-in-backup-plan	Untuk membantu proses pencadang an data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (2)	Situs Penyimpan an Alternatif | Waktu Pemulihan dan Tujuan Titik Pemulihan	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (2)	Situs Penyimpan an Alternatif | Waktu Pemulihan dan Tujuan Titik Pemulihan	efs-in-backup-plan	Untuk membantu proses pencadang an data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (2)	Situs Penyimpanan Alternatif | Waktu Pemulihan dan Tujuan Titik Pemulihan	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (2)	Situs Penyimpanan Alternatif | Waktu Pemulihan dan Tujuan Titik Pemulihan	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (2)	Situs Penyimpan an Alternatif | Waktu Pemulihan dan Tujuan Titik Pemulihan	s3- version-lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihk an objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).
CP-6 (2)	Situs Penyimpan an Alternatif | Waktu Pemulihan dan Tujuan Titik Pemulihan	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (2)	Situs Penyimpanan Alternatif | Waktu Pemulihan dan Tujuan Titik Pemulihan	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (2)	Situs Penyimpanan Alternatif | Waktu Pemulihan dan Tujuan Titik Pemulihan	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan cadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (2)	Situs Penyimpanan Alternatif | Waktu Pemulihan dan Tujuan Titik Pemulihan	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (2)	Situs Penyimpanan Alternatif | Waktu Pemulihan dan Tujuan Titik Pemulihan	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (2)	Situs Penyimpanan Alternatif | Waktu Pemulihan dan Tujuan Titik Pemulihan	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (2)	Situs Penyimpan an Alternatif | Waktu Pemulihan dan Tujuan Titik Pemulihan	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6 (2)	Situs Penyimpanan Alternatif | Waktu Pemulihan dan Tujuan Titik Pemulihan	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6	Situs Penyimpanan Alternatif	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6	Situs Penyimpanan Alternatif	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6	Situs Penyimpanan Alternatif	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6	Situs Penyimpanan Alternatif	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6	Situs Penyimpanan Alternatif	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6	Situs Penyimpanan Alternatif	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6	Situs Penyimpanan Alternatif	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-6	Situs Penyimpanan Alternatif	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	Sistem Backup	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	Sistem Backup	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	Sistem Backup	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	Sistem Backup	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	Sistem Backup	s3- version-lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihkan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).
CP-9	Sistem Backup	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	Sistem Backup	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan cadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	Sistem Backup	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	Sistem Backup	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	Sistem Backup	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	Sistem Backup	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-9	Sistem Backup	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Pemulihan dan Rekonstitusi Sistem	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Pemulihan dan Rekonstitusi Sistem	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Pemulihan dan Rekonstitusi Sistem	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Pemulihan dan Rekonstitusi Sistem	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Pemulihan dan Rekonstitusi Sistem	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Pemulihan dan Rekonstitusi Sistem	s3- version-lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihkan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).
CP-10	Pemulihan dan Rekonstitusi Sistem	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Pemulihan dan Rekonstitusi Sistem	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Pemulihan dan Rekonstitusi Sistem	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan cadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Pemulihan dan Rekonstitusi Sistem	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Pemulihan dan Rekonstitusi Sistem	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Pemulihan dan Rekonstitusi Sistem	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Pemulihan dan Rekonstitusi Sistem	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Pemulihan dan Rekonstitusi Sistem	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CP-10	Pemulihan dan Rekonstitusi Sistem	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2 (1)	Identifikasi dan Otentikasi (Pengguna organisasi) | Otentikasi Multi-faktor ke Akun Istimewa	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2 (1)	Identifikasi dan Otentikasi (Pengguna organisasi) | Otentikasi Multi-faktor ke Akun Istimewa	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2 (1)	Identifikasi dan Otentikasi (Pengguna organisasi) | Otentikasi Multi-faktor ke Akun Istimewa	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2 (1)	Identifikasi dan Otentikasi (Pengguna organisasi) | Otentikasi Multi-faktor ke Akun Istimewa	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2 (2)	Identifikasi dan Otentikasi (Pengguna organisasi) | Otentikasi Multi-faktor ke Akun Non-Privileged	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2 (2)	Identifikasi dan Otentikasi (Pengguna organisasi) | Otentikasi Multi-faktor ke Akun Non-Privileged	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2 (2)	Identifikasi dan Otentikasi (Pengguna organisasi) | Otentikasi Multi-faktor ke Akun Non-Privileged	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2 (2)	Identifikasi dan Otentikasi (Pengguna organisasi) | Otentikasi Multi-faktor ke Akun Non-Privileged	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2 (6)	Identifikasi dan Otentikasi (Pengguna organisasi) | Akses ke Akun —Perangkat terpisah	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2 (6)	Identifikasi dan Otentikasi (Pengguna organisasi) | Akses ke Akun —Perangkat terpisah	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2 (6)	Identifikasi dan Otentikasi (Pengguna organisasi) | Akses ke Akun —Perangkat terpisah	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2 (6)	Identifikasi dan Otentikasi (Pengguna organisasi) | Akses ke Akun —Perangkat terpisah	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2 (8)	Identifikasi dan Otentikasi (Pengguna organisasi) | Akses ke Akun - Replay Resistant	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2 (8)	Identifikasi dan Otentikasi (Pengguna organisasi) | Akses ke Akun - Replay Resistant	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2 (8)	Identifikasi dan Otentikasi (Pengguna organisasi) | Akses ke Akun - Replay Resistant	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-2 (8)	Identifikasi dan Otentikasi (Pengguna organisasi) | Akses ke Akun - Replay Resistant	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
IA-5 (1)	Manajemen Authenticator | Otentikasi Berbasis Kata Sandi	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-5 (1)	Manajemen Authenticator | Otentikasi Berbasis Kata Sandi	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
IA-5 (1)	Manajemen Authenticator | Otentikasi Berbasis Kata Sandi	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-5 (1)	Manajemen Authenticator | Otentikasi Berbasis Kata Sandi	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.
IA-5 (1)	Manajemen Authenticator | Otentikasi Berbasis Kata Sandi	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-5 (1)	Manajemen Authenticator | Otentikasi Berbasis Kata Sandi	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-5 (1)	Manajemen Authenticator | Otentikasi Berbasis Kata Sandi	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-5 (1)	Manajemen Authenticator | Otentikasi Berbasis Kata Sandi	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IA-5 (7)	Manajemen Authenticator | Tidak Ada Authenticator Statis Tidak Terenkripsi Tertanam	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild . Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-4 (1)	Penanganan Insiden | Proses Penanganan Insiden Otomatis	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
IR-4 (5)	Penanganan Insiden | Penonaktifan Sistem Secara Otomatis	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RA-3 (4)	Penilaian Risiko | Analisis Cyber Prediktif	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-3	Siklus Hidup Pengembangan Sistem	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild . Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-3	Siklus Hidup Pengembangan Sistem	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-8 (19)	Prinsip Rekayasa Keamanan dan Privasi | Perlindungan Berkelanjutan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-8 (21)	Prinsip Rekayasa Keamanan dan Privasi | Analisis diri	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-8 (22)	Prinsip Rekayasa Keamanan dan Privasi | Akuntabilitas dan Keterlacakan	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-8 (25)	Prinsip Rekayasa Keamanan dan Privasi | Keamanan Ekonomi	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-11 (1)	Pengujian dan Evaluasi Pengembang | Analisis Kode Statis	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-11 (6)	Pengujian dan Evaluasi Pengembang | Ulasan Attack Surface	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-15 (2)	Proses Pengembangan, Standar, dan Alat | Alat Pelacakan Keamanan dan Privasi	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-15 (2)	Proses Pengembangan, Standar, dan Alat | Alat Pelacakan Keamanan dan Privasi	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-15 (8)	Proses Pengembangan, Standar, dan Alat | Penggunaan Kembali Informasi Ancaman dan Kerentanan	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SA-15 (8)	Proses Pengembangan, Standar, dan Alat | Penggunaan Kembali Informasi Ancaman dan Kerentanan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5 (1)	Denial-of-service Perlindungan | Batasi Kemampuan untuk Menyerang Sistem Lain	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5 (2)	Denial-of-service Perlindungan | Kapasitas, Bandwidth, dan Redundansi	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5 (2)	Denial-of-service Perlindungan | Kapasitas, Bandwidth, dan Redundansi	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5 (2)	Denial-of-service Perlindungan | Kapasitas, Bandwidth, dan Redundansi	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5 (2)	Denial-of-service Perlindungan | Kapasitas, Bandwidth, dan Redundansi	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5 (2)	Denial-of-service Perlindungan | Kapasitas, Bandwidth, dan Redundansi	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relationa l Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindun gan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersedi aan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5 (2)	Denial-of-service Perlindungan | Kapasitas, Bandwidth, dan Redundansi	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5 (2)	Denial-of-service Perlindungan | Kapasitas, Bandwidth, dan Redundansi	s3- version-lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihkan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).
SC-5 (2)	Denial-of-service Perlindungan | Kapasitas, Bandwidth, dan Redundansi	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5 (2)	Denial-of-service Perlindungan | Kapasitas, Bandwidth, dan Redundansi	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5 (2)	Denial-of-service Perlindungan | Kapasitas, Bandwidth, dan Redundansi	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan cadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5 (2)	Denial-of-service Perlindungan | Kapasitas, Bandwidth, dan Redundansi	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5 (2)	Denial-of-service Perlindungan | Kapasitas, Bandwidth, dan Redundansi	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5 (2)	Denial-of-service Perlindungan | Kapasitas, Bandwidth, dan Redundansi	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5 (2)	Denial-of-service Perlindungan | Kapasitas, Bandwidth, dan Redundansi	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5 (2)	Denial-of-service Perlindungan | Kapasitas, Bandwidth, dan Redundansi	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5 (2)	Denial-of-service Perlindungan | Kapasitas, Bandwidth, dan Redundansi	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5 (2)	Denial-of-service Perlindungan | Kapasitas, Bandwidth, dan Redundansi	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5 (2)	Denial-of-service Perlindungan | Kapasitas, Bandwidth, dan Redundansi	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimpleme ntasikan untuk mencapai persyarat an ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivi tas jika salah satu koneksi Site-to-S ite VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivi tas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5 (3)	Denial-of-service Perlindungan | Deteksi dan Pemantauan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-5	Denial-of-service Perlindungan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Perlindungan Batas | Titik Akses	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Perlindungan Batas | Titik Akses	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Perlindungan Batas | Titik Akses	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
SC-7 (3)	Perlindungan Batas | Titik Akses	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Perlindungan Batas | Titik Akses	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
SC-7 (3)	Perlindungan Batas | Titik Akses	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Perlindungan Batas | Titik Akses	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
SC-7 (3)	Perlindungan Batas | Titik Akses	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Perlindungan Batas | Titik Akses	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Perlindungan Batas | Titik Akses	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Perlindungan Batas | Titik Akses	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Perlindungan Batas | Titik Akses	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
SC-7 (3)	Perlindungan Batas | Titik Akses	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Perlindungan Batas | Titik Akses	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Perlindungan Batas | Titik Akses	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Perlindungan Batas | Titik Akses	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
SC-7 (3)	Perlindungan Batas | Titik Akses	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Perlindungan Batas | Titik Akses	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
SC-7 (3)	Perlindungan Batas | Titik Akses	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (3)	Perlindungan Batas | Titik Akses	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositori data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigurasi ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (4)	Perlindungan Batas | Layanan Telekomunikasi Eksternal	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (5)	Perlindungan Batas | Tolak secara Default - Izinkan dengan Pengecualian	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (5)	Perlindungan Batas | Tolak secara Default - Izinkan dengan Pengecualian	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (5)	Perlindungan Batas | Tolak secara Default - Izinkan dengan Pengecualian	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (5)	Perlindungan Batas | Tolak secara Default - Izinkan dengan Pengecualian	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositor i data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
SC-7 (9)	Perlindungan Batas | Batasi Ancaman Lalu Lintas Komunikasi Keluar	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (10)	Perlindungan Batas | Cegah Eksfiltrasi	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
SC-7 (10)	Perlindungan Batas | Cegah Eksfiltrasi	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (10)	Perlindungan Batas | Cegah Eksfiltrasi	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-7 (10)	Perlindungan Batas | Cegah Eksfiltrasi	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
SC-7 (10)	Perlindungan Batas | Cegah Eksfiltrasi	elasticsearch-encr ypted-at-rest	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk domain OpenSearc h Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (10)	Perlindungan Batas | Cegah Eksfiltrasi	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
SC-7 (10)	Perlindungan Batas | Cegah Eksfiltrasi	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (10)	Perlindungan Batas | Cegah Eksfiltrasi	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-7 (10)	Perlindungan Batas | Cegah Eksfiltrasi	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (10)	Perlindungan Batas | Cegah Eksfiltrasi	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (10)	Perlindungan Batas | Cegah Eksfiltrasi	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (10)	Perlindungan Batas | Cegah Eksfiltrasi	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
SC-7 (10)	Perlindungan Batas | Cegah Eksfiltrasi	s3- default-encryption -kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (10)	Perlindungan Batas | Cegah Eksfiltrasi	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-7 (10)	Perlindungan Batas | Cegah Eksfiltrasi	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (10)	Perlindungan Batas | Cegah Eksfiltrasi	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (10)	Perlindungan Batas | Cegah Eksfiltrasi	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
SC-7 (10)	Perlindungan Batas | Cegah Eksfiltrasi	kinesis-stream-encrypted	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (11)	Perlindungan Batas | Batasi Lalu Lintas Komunikasi Masuk	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (11)	Perlindungan Batas | Batasi Lalu Lintas Komunikasi Masuk	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (11)	Perlindungan Batas | Batasi Lalu Lintas Komunikasi Masuk	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (11)	Perlindungan Batas | Batasi Lalu Lintas Komunikasi Masuk	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
SC-7 (11)	Perlindungan Batas | Batasi Lalu Lintas Komunikasi Masuk	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositor i data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (11)	Perlindungan Batas | Batasi Lalu Lintas Komunikasi Masuk	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
SC-7 (11)	Perlindungan Batas | Batasi Lalu Lintas Komunikasi Masuk	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (11)	Perlindungan Batas | Batasi Lalu Lintas Komunikasi Masuk	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
SC-7 (11)	Perlindungan Batas | Batasi Lalu Lintas Komunikasi Masuk	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (11)	Perlindungan Batas | Batasi Lalu Lintas Komunikasi Masuk	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
SC-7 (11)	Perlindungan Batas | Batasi Lalu Lintas Komunikasi Masuk	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (11)	Perlindungan Batas | Batasi Lalu Lintas Komunikasi Masuk	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (11)	Perlindungan Batas | Batasi Lalu Lintas Komunikasi Masuk	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (11)	Perlindungan Batas | Batasi Lalu Lintas Komunikasi Masuk	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (11)	Perlindungan Batas | Batasi Lalu Lintas Komunikasi Masuk	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
SC-7 (11)	Perlindungan Batas | Batasi Lalu Lintas Komunikasi Masuk	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (11)	Perlindungan Batas | Batasi Lalu Lintas Komunikasi Masuk	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (11)	Perlindungan Batas | Batasi Lalu Lintas Komunikasi Masuk	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (11)	Perlindungan Batas | Batasi Lalu Lintas Komunikasi Masuk	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (11)	Perlindungan Batas | Batasi Lalu Lintas Komunikasi Masuk	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
SC-7 (11)	Perlindungan Batas | Batasi Lalu Lintas Komunikasi Masuk	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (11)	Perlindungan Batas | Batasi Lalu Lintas Komunikasi Masuk	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
SC-7 (11)	Perlindungan Batas | Batasi Lalu Lintas Komunikasi Masuk	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (11)	Perlindungan Batas | Batasi Lalu Lintas Komunikasi Masuk	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (11)	Perlindungan Batas | Batasi Lalu Lintas Komunikasi Masuk	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (11)	Perlindungan Batas | Batasi Lalu Lintas Komunikasi Masuk	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (16)	Perlindungan Batas | Mencegah Penemuan Komponen Sistem	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (16)	Perlindungan Batas | Mencegah Penemuan Komponen Sistem	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (16)	Perlindungan Batas | Mencegah Penemuan Komponen Sistem	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (16)	Perlindungan Batas | Mencegah Penemuan Komponen Sistem	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
SC-7 (16)	Perlindungan Batas | Mencegah Penemuan Komponen Sistem	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (16)	Perlindungan Batas | Mencegah Penemuan Komponen Sistem	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
SC-7 (16)	Perlindungan Batas | Mencegah Penemuan Komponen Sistem	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (16)	Perlindungan Batas | Mencegah Penemuan Komponen Sistem	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
SC-7 (16)	Perlindungan Batas | Mencegah Penemuan Komponen Sistem	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (16)	Perlindungan Batas | Mencegah Penemuan Komponen Sistem	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
SC-7 (16)	Perlindungan Batas | Mencegah Penemuan Komponen Sistem	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (16)	Perlindungan Batas | Mencegah Penemuan Komponen Sistem	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (16)	Perlindungan Batas | Mencegah Penemuan Komponen Sistem	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (16)	Perlindungan Batas | Mencegah Penemuan Komponen Sistem	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (16)	Perlindungan Batas | Mencegah Penemuan Komponen Sistem	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
SC-7 (16)	Perlindungan Batas | Mencegah Penemuan Komponen Sistem	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (16)	Perlindungan Batas | Mencegah Penemuan Komponen Sistem	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (16)	Perlindungan Batas | Mencegah Penemuan Komponen Sistem	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (16)	Perlindungan Batas | Mencegah Penemuan Komponen Sistem	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (16)	Perlindungan Batas | Mencegah Penemuan Komponen Sistem	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
SC-7 (16)	Perlindungan Batas | Mencegah Penemuan Komponen Sistem	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (16)	Perlindungan Batas | Mencegah Penemuan Komponen Sistem	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
SC-7 (16)	Perlindungan Batas | Mencegah Penemuan Komponen Sistem	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (16)	Perlindungan Batas | Mencegah Penemuan Komponen Sistem	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (16)	Perlindungan Batas | Mencegah Penemuan Komponen Sistem	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (16)	Perlindungan Batas | Mencegah Penemuan Komponen Sistem	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (21)	Perlindungan Batas | Isolasi Komponen Sistem	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (21)	Perlindungan Batas | Isolasi Komponen Sistem	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (21)	Perlindungan Batas | Isolasi Komponen Sistem	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (21)	Perlindungan Batas | Isolasi Komponen Sistem	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
SC-7 (21)	Perlindungan Batas | Isolasi Komponen Sistem	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositor i data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (21)	Perlindungan Batas | Isolasi Komponen Sistem	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
SC-7 (21)	Perlindungan Batas | Isolasi Komponen Sistem	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (21)	Perlindungan Batas | Isolasi Komponen Sistem	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
SC-7 (21)	Perlindungan Batas | Isolasi Komponen Sistem	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (21)	Perlindungan Batas | Isolasi Komponen Sistem	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
SC-7 (21)	Perlindungan Batas | Isolasi Komponen Sistem	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (21)	Perlindungan Batas | Isolasi Komponen Sistem	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (21)	Perlindungan Batas | Isolasi Komponen Sistem	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (21)	Perlindungan Batas | Isolasi Komponen Sistem	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (21)	Perlindungan Batas | Isolasi Komponen Sistem	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
SC-7 (21)	Perlindungan Batas | Isolasi Komponen Sistem	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (21)	Perlindungan Batas | Isolasi Komponen Sistem	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (21)	Perlindungan Batas | Isolasi Komponen Sistem	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (21)	Perlindungan Batas | Isolasi Komponen Sistem	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (21)	Perlindungan Batas | Isolasi Komponen Sistem	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
SC-7 (21)	Perlindungan Batas | Isolasi Komponen Sistem	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (21)	Perlindungan Batas | Isolasi Komponen Sistem	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
SC-7 (21)	Perlindungan Batas | Isolasi Komponen Sistem	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (21)	Perlindungan Batas | Isolasi Komponen Sistem	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (21)	Perlindungan Batas | Isolasi Komponen Sistem	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7 (21)	Perlindungan Batas | Isolasi Komponen Sistem	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Perlindungan Batas	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Perlindungan Batas	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Perlindungan Batas	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Perlindungan Batas	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
SC-7	Perlindungan Batas	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositor i data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Perlindungan Batas	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
SC-7	Perlindungan Batas	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Perlindungan Batas	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
SC-7	Perlindungan Batas	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Perlindungan Batas	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
SC-7	Perlindungan Batas	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Perlindungan Batas	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Perlindungan Batas	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Perlindungan Batas	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Perlindungan Batas	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
SC-7	Perlindungan Batas	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Perlindungan Batas	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Perlindungan Batas	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Perlindungan Batas	s3- account-level-publ ic-access -blok-per iodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Perlindungan Batas	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
SC-7	Perlindungan Batas	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Perlindungan Batas	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
SC-7	Perlindungan Batas	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Perlindungan Batas	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Perlindungan Batas	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-7	Perlindungan Batas	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8 (1)	Kerahasiaan dan Integritas Transmisi | Perlindungan Kriptografi	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8 (1)	Kerahasiaan dan Integritas Transmisi | Perlindungan Kriptografi	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
SC-8 (1)	Kerahasiaan dan Integritas Transmisi | Perlindungan Kriptografi	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8 (1)	Kerahasiaan dan Integritas Transmisi | Perlindungan Kriptografi	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
SC-8 (1)	Kerahasiaan dan Integritas Transmisi | Perlindungan Kriptografi	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8 (1)	Kerahasiaan dan Integritas Transmisi | Perlindungan Kriptografi	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-8 (1)	Kerahasiaan dan Integritas Transmisi | Perlindungan Kriptografi	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8 (1)	Kerahasiaan dan Integritas Transmisi | Perlindungan Kriptografi	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
SC-8 (1)	Kerahasiaan dan Integritas Transmisi | Perlindungan Kriptografi	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8 (1)	Kerahasiaan dan Integritas Transmisi | Perlindungan Kriptografi	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8 (2)	Kerahasiaan dan Integritas Transmisi | Penanganan Pra dan Pasca Transmisi	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-8 (2)	Kerahasiaan dan Integritas Transmisi | Penanganan Pra dan Pasca Transmisi	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8 (2)	Kerahasiaan dan Integritas Transmisi | Penanganan Pra dan Pasca Transmisi	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
SC-8 (2)	Kerahasiaan dan Integritas Transmisi | Penanganan Pra dan Pasca Transmisi	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8 (2)	Kerahasiaan dan Integritas Transmisi | Penanganan Pra dan Pasca Transmisi	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan Applicati on Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-8 (2)	Kerahasiaan dan Integritas Transmisi | Penanganan Pra dan Pasca Transmisi	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8 (2)	Kerahasiaan dan Integritas Transmisi | Penanganan Pra dan Pasca Transmisi	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8 (2)	Kerahasiaan dan Integritas Transmisi | Penanganan Pra dan Pasca Transmisi	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
SC-8 (2)	Kerahasiaan dan Integritas Transmisi | Penanganan Pra dan Pasca Transmisi	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8 (2)	Kerahasiaan dan Integritas Transmisi | Penanganan Pra dan Pasca Transmisi	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8	Kerahasiaan dan Integritas Transmisi	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8	Kerahasiaan dan Integritas Transmisi	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
SC-8	Kerahasiaan dan Integritas Transmisi	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8	Kerahasiaan dan Integritas Transmisi	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
SC-8	Kerahasiaan dan Integritas Transmisi	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8	Kerahasiaan dan Integritas Transmisi	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan Applicati on Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-8	Kerahasiaan dan Integritas Transmisi	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8	Kerahasiaan dan Integritas Transmisi	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
SC-8	Kerahasiaan dan Integritas Transmisi	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-8	Kerahasiaan dan Integritas Transmisi	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-12 (2)	Pembentukan dan Manajemen Kunci Kriptografi | Kunci Simetris	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-12 (2)	Pembentukan dan Manajemen Kunci Kriptografi | Kunci Simetris	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-12 (3)	Pembentukan dan Manajemen Kunci Kriptografi | Kunci Asimetris	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
SC-12 (3)	Pembentukan dan Manajemen Kunci Kriptografi | Kunci Asimetris	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-12 (3)	Pembentukan dan Manajemen Kunci Kriptografi | Kunci Asimetris	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
SC-12 (3)	Pembentukan dan Manajemen Kunci Kriptografi | Kunci Asimetris	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-12 (3)	Pembentukan dan Manajemen Kunci Kriptografi | Kunci Asimetris	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
SC-12 (3)	Pembentukan dan Manajemen Kunci Kriptografi | Kunci Asimetris	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-12 (3)	Pembentukan dan Manajemen Kunci Kriptografi | Kunci Asimetris	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-12	Pembentukan dan Manajemen Kunci Kriptografi	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-12	Pembentukan dan Manajemen Kunci Kriptografi	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.
SC-13	Perlindungan Kriptografi	codebuild-project-artifact-encryption	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk AWS CodeBuild artefak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13	Perlindungan Kriptografi	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
SC-13	Perlindungan Kriptografi	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13	Perlindungan Kriptografi	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-13	Perlindungan Kriptografi	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13	Perlindungan Kriptografi	kinesis-stream-encrypted	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.
SC-13	Perlindungan Kriptografi	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13	Perlindungan Kriptografi	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-13	Perlindungan Kriptografi	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13	Perlindungan Kriptografi	s3- default-encryption -kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-13	Perlindungan Kriptografi	sagemaker-notebook -instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13	Perlindungan Kriptografi	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13	Perlindungan Kriptografi	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan Applicati on Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-13	Perlindungan Kriptografi	api-gw-cache-enabl ed-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13	Perlindungan Kriptografi	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
SC-13	Perlindungan Kriptografi	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrai l jejak Anda.
SC-13	Perlindungan Kriptografi	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13	Perlindungan Kriptografi	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
SC-13	Perlindungan Kriptografi	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13	Perlindungan Kriptografi	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
SC-13	Perlindungan Kriptografi	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13	Perlindungan Kriptografi	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
SC-13	Perlindungan Kriptografi	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13	Perlindungan Kriptografi	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDbEncrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13	Perlindungan Kriptografi	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-13	Perlindungan Kriptografi	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13	Perlindungan Kriptografi	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
SC-13	Perlindungan Kriptografi	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-13	Perlindungan Kriptografi	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-13	Perlindungan Kriptografi	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-23 (3)	Keaslian Sesi | Pengidentifikasi Sesi yang Dihasilkan Sistem Unik	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-23 (3)	Keaslian Sesi | Pengidentifikasi Sesi yang Dihasilkan Sistem Unik	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-23 (3)	Keaslian Sesi | Pengidentifikasi Sesi yang Dihasilkan Sistem Unik	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
SC-23 (3)	Keaslian Sesi | Pengidentifikasi Sesi yang Dihasilkan Sistem Unik	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-23 (3)	Keaslian Sesi | Pengidentifikasi Sesi yang Dihasilkan Sistem Unik	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan Applicati on Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-23 (3)	Keaslian Sesi | Pengidentifikasi Sesi yang Dihasilkan Sistem Unik	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-23 (3)	Keaslian Sesi | Pengidentifikasi Sesi yang Dihasilkan Sistem Unik	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
SC-23 (3)	Keaslian Sesi | Pengidentifikasi Sesi yang Dihasilkan Sistem Unik	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-23 (3)	Keaslian Sesi | Pengidentifikasi Sesi yang Dihasilkan Sistem Unik	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-23 (5)	Keaslian Sesi | Otoritas Sertifikat yang Diizinkan	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-23 (5)	Keaslian Sesi | Otoritas Sertifikat yang Diizinkan	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-23	Keaslian Sesi	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-23	Keaslian Sesi	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-23	Keaslian Sesi	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
SC-23	Keaslian Sesi	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-23	Keaslian Sesi	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan Applicati on Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-23	Keaslian Sesi	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-23	Keaslian Sesi	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-23	Keaslian Sesi	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
SC-23	Keaslian Sesi	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-23	Keaslian Sesi	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SC-28 (1)	Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	codebuild-project-artifact-encryption	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk AWS CodeBuild artefak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28 (1)	Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
SC-28 (1)	Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28 (1)	Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	kinesis-stream-encrypted	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.
SC-28 (1)	Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-28 (1)	Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28 (1)	Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28 (1)	Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-28 (1)	Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28 (1)	Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
SC-28 (1)	Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
SC-28 (1)	Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28 (1)	Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
SC-28 (1)	Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
SC-28 (1)	Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28 (1)	Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28 (1)	Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-28 (1)	Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28 (1)	Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-28 (1)	Perlindungan Informasi Saat Istirahat | Perlindungan Kriptografi	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28 (3)	Perlindungan Informasi Saat Istirahat | Kunci Kriptografi	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
SC-28 (3)	Perlindungan Informasi Saat Istirahat | Kunci Kriptografi	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.
SC-28	Perlindungan Informasi Saat Istirahat	codebuild-project-artifact-encryption	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk AWS CodeBuild artefak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28	Perlindungan Informasi Saat Istirahat	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
SC-28	Perlindungan Informasi Saat Istirahat	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28	Perlindungan Informasi Saat Istirahat	kinesis-stream-encrypted	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.
SC-28	Perlindungan Informasi Saat Istirahat	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-28	Perlindungan Informasi Saat Istirahat	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28	Perlindungan Informasi Saat Istirahat	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28	Perlindungan Informasi Saat Istirahat	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-28	Perlindungan Informasi Saat Istirahat	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28	Perlindungan Informasi Saat Istirahat	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
SC-28	Perlindungan Informasi Saat Istirahat	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
SC-28	Perlindungan Informasi Saat Istirahat	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28	Perlindungan Informasi Saat Istirahat	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
SC-28	Perlindungan Informasi Saat Istirahat	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
SC-28	Perlindungan Informasi Saat Istirahat	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28	Perlindungan Informasi Saat Istirahat	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28	Perlindungan Informasi Saat Istirahat	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-28	Perlindungan Informasi Saat Istirahat	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-28	Perlindungan Informasi Saat Istirahat	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SC-28	Perlindungan Informasi Saat Istirahat	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-36 (2)	Pemrosesan dan Penyimpanan Terdistribusi | Sinkronisasi	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-36	Pemrosesan dan Penyimpanan Terdistribusi	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-36	Pemrosesan dan Penyimpanan Terdistribusi	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-36	Pemrosesan dan Penyimpanan Terdistribusi	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SC-36	Pemrosesan dan Penyimpanan Terdistribusi	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2 (2)	Remediasi Cacat | Status Remediasi Cacat Otomatis	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
SI-2 (2)	Remediasi Cacat | Status Remediasi Cacat Otomatis	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2 (2)	Remediasi Cacat | Status Remediasi Cacat Otomatis	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2 (3)	Remediasi Cacat | Saatnya Memperbaiki Kelemahan dan Tolok Ukur untuk Tindakan Korektif	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2 (3)	Remediasi Cacat | Saatnya Memperbaiki Kelemahan dan Tolok Ukur untuk Tindakan Korektif	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi ke instans terkelola Anda dan memungkinkan Anda untuk menetapkan garis dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2 (3)	Remediasi Cacat | Saatnya Memperbaiki Kelemahan dan Tolok Ukur untuk Tindakan Korektif	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2 (4)	Remediasi Cacat | Alat Manajemen Patch Otomatis	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
SI-2 (4)	Remediasi Cacat | Alat Manajemen Patch Otomatis	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2 (4)	Remediasi Cacat | Alat Manajemen Patch Otomatis	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2 (5)	Remediasi Cacat | Pembaruan Perangkat Lunak dan Firmware Otomatis	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
SI-2 (5)	Remediasi Cacat | Pembaruan Perangkat Lunak dan Firmware Otomatis	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2 (5)	Remediasi Cacat | Pembaruan Perangkat Lunak dan Firmware Otomatis	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2	Remediasi Cacat	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2	Remediasi Cacat	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2	Remediasi Cacat	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2	Remediasi Cacat	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2	Remediasi Cacat	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2	Remediasi Cacat	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
SI-2	Remediasi Cacat	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2	Remediasi Cacat	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-2	Remediasi Cacat	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-3 (8)	Perlindungan Kode Berbahaya | Mendeteksi Perintah Tidak Sah	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-3 (8)	Perlindungan Kode Berbahaya | Mendeteksi Perintah Tidak Sah	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-3 (8)	Perlindungan Kode Berbahaya | Mendeteksi Perintah Tidak Sah	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.
SI-3 (8)	Perlindungan Kode Berbahaya | Mendeteksi Perintah Tidak Sah	s3- event-notification s-enabled	Pemberitahuan peristiwa Amazon S3 dapat memberi tahu personel terkait tentang modifikasi yang tidak disengaja atau disengaja pada objek bucket Anda. Contoh peringatan meliputi: objek baru adalah pembuatan, penghapusan objek, restorasi objek, objek yang hilang dan direplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-3 (8)	Perlindungan Kode Berbahaya | Mendeteksi Perintah Tidak Sah	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
SI-3 (8)	Perlindungan Kode Berbahaya | Mendeteksi Perintah Tidak Sah	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-3 (8)	Perlindungan Kode Berbahaya | Mendeteksi Perintah Tidak Sah	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
SI-3 (8)	Perlindungan Kode Berbahaya | Mendeteksi Perintah Tidak Sah	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-3 (8)	Perlindungan Kode Berbahaya | Mendeteksi Perintah Tidak Sah	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-3 (8)	Perlindungan Kode Berbahaya | Mendeteksi Perintah Tidak Sah	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-3 (8)	Perlindungan Kode Berbahaya | Mendeteksi Perintah Tidak Sah	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (1)	Pemantauan Sistem | Sistem Deteksi Intrusi Seluruh Sistem	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (2)	Pemantauan Sistem | Alat dan Mekanisme Otomatis untuk Analisis Waktu Nyata	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
SI-4 (4)	Pemantauan Sistem | Lalu Lintas Komunikasi Masuk dan Keluar	s3- event-notifications-enabled	Pemberitahuan peristiwa Amazon S3 dapat memberi tahu personel terkait tentang modifikasi yang tidak disengaja atau disengaja pada objek bucket Anda. Contoh peringatan meliputi: objek baru adalah pembuatan, penghapusan objek, restorasi objek, objek yang hilang dan direplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (4)	Pemantauan Sistem | Lalu Lintas Komunikasi Masuk dan Keluar	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (5)	Pemantauan Sistem | Peringatan yang dihasilkan sistem	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (5)	Pemantauan Sistem | Peringatan yang dihasilkan sistem	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
SI-4 (5)	Pemantauan Sistem | Peringatan yang dihasilkan sistem	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (12)	Pemantauan Sistem | Peringatan yang dihasilkan Organisasi Otomatis	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (13)	Pemantauan Sistem | Menganalisis Lalu Lintas dan Pola Peristiwa	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (20)	Pemantauan Sistem | Pengguna Istimewa	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (20)	Pemantauan Sistem | Pengguna Istimewa	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (20)	Pemantauan Sistem | Pengguna Istimewa	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.
SI-4 (20)	Pemantauan Sistem | Pengguna Istimewa	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (20)	Pemantauan Sistem | Pengguna Istimewa	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
SI-4 (20)	Pemantauan Sistem | Pengguna Istimewa	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (20)	Pemantauan Sistem | Pengguna Istimewa	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (20)	Pemantauan Sistem | Pengguna Istimewa	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (20)	Pemantauan Sistem | Pengguna Istimewa	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (22)	Pemantauan Sistem | Layanan Jaringan Tidak Resmi	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4 (25)	Pemantauan Sistem | Optimalkan Analisis Lalu Lintas Jaringan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
SI-4	Pemantauan Sistem	s3- event-notifications-enabled	Pemberitahuan peristiwa Amazon S3 dapat memberi tahu personel terkait tentang modifikasi yang tidak disengaja atau disengaja pada objek bucket Anda. Contoh peringatan meliputi: objek baru adalah pembuatan, penghapusan objek, restorasi objek, objek yang hilang dan direplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4	Pemantauan Sistem	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-4	Pemantauan Sistem	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (1)	Perangkat Lunak, Firmware, dan Integritas Informasi | Pemeriksaan Integrita s	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (3)	Perangkat Lunak, Firmware, dan Integritas Informasi | Alat Integritas yang Dikelola Secara Terpusat	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.
SI-7 (6)	Perangkat Lunak, Firmware, dan Integritas Informasi | Perlindungan Kriptografi	codebuild-project-artifact-encryption	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk AWS CodeBuild artefak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (6)	Perangkat Lunak, Firmware, dan Integritas Informasi | Perlindungan Kriptografi	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
SI-7 (6)	Perangkat Lunak, Firmware, dan Integritas Informasi | Perlindungan Kriptografi	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (6)	Perangkat Lunak, Firmware, dan Integritas Informasi | Perlindungan Kriptografi	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
SI-7 (6)	Perangkat Lunak, Firmware, dan Integritas Informasi | Perlindungan Kriptografi	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (6)	Perangkat Lunak, Firmware, dan Integritas Informasi | Perlindungan Kriptografi	kinesis-stream-encrypted	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.
SI-7 (6)	Perangkat Lunak, Firmware, dan Integritas Informasi | Perlindungan Kriptografi	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
SI-7 (6)	Perangkat Lunak, Firmware, dan Integritas Informasi | Perlindungan Kriptografi	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (6)	Perangkat Lunak, Firmware, dan Integritas Informasi | Perlindungan Kriptografi	s3- default-encryption -kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SI-7 (6)	Perangkat Lunak, Firmware, dan Integritas Informasi | Perlindungan Kriptografi	sagemaker-notebook -instance-kms-kunci- dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (6)	Perangkat Lunak, Firmware, dan Integritas Informasi | Perlindungan Kriptografi	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (6)	Perangkat Lunak, Firmware, dan Integritas Informasi | Perlindungan Kriptografi	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan Applicati on Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SI-7 (6)	Perangkat Lunak, Firmware, dan Integritas Informasi | Perlindungan Kriptografi	api-gw-cache-enabl ed-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (6)	Perangkat Lunak, Firmware, dan Integritas Informasi | Perlindungan Kriptografi	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
SI-7 (6)	Perangkat Lunak, Firmware, dan Integritas Informasi | Perlindungan Kriptografi	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrai l jejak Anda.
SI-7 (6)	Perangkat Lunak, Firmware, dan Integritas Informasi | Perlindungan Kriptografi	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (6)	Perangkat Lunak, Firmware, dan Integritas Informasi | Perlindungan Kriptografi	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
SI-7 (6)	Perangkat Lunak, Firmware, dan Integritas Informasi | Perlindungan Kriptografi	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (6)	Perangkat Lunak, Firmware, dan Integritas Informasi | Perlindungan Kriptografi	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
SI-7 (6)	Perangkat Lunak, Firmware, dan Integritas Informasi | Perlindungan Kriptografi	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
SI-7 (6)	Perangkat Lunak, Firmware, dan Integritas Informasi | Perlindungan Kriptografi	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (6)	Perangkat Lunak, Firmware, dan Integritas Informasi | Perlindungan Kriptografi	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (6)	Perangkat Lunak, Firmware, dan Integritas Informasi | Perlindungan Kriptografi	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
SI-7 (6)	Perangkat Lunak, Firmware, dan Integritas Informasi | Perlindungan Kriptografi	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (6)	Perangkat Lunak, Firmware, dan Integritas Informasi | Perlindungan Kriptografi	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
SI-7 (6)	Perangkat Lunak, Firmware, dan Integritas Informasi | Perlindungan Kriptografi	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (6)	Perangkat Lunak, Firmware, dan Integritas Informasi | Perlindungan Kriptografi	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (7)	Perangkat Lunak, Firmware, dan Integritas Informasi | Integrasi Deteksi dan Respon	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (8)	Perangkat Lunak, Firmware, dan Integritas Informasi | Kemampuan Audit untuk Peristiwa Penting	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (8)	Perangkat Lunak, Firmware, dan Integritas Informasi | Kemampuan Audit untuk Peristiwa Penting	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (8)	Perangkat Lunak, Firmware, dan Integritas Informasi | Kemampuan Audit untuk Peristiwa Penting	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (8)	Perangkat Lunak, Firmware, dan Integritas Informasi | Kemampuan Audit untuk Peristiwa Penting	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
SI-7 (8)	Perangkat Lunak, Firmware, dan Integritas Informasi | Kemampuan Audit untuk Peristiwa Penting	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (8)	Perangkat Lunak, Firmware, dan Integritas Informasi | Kemampuan Audit untuk Peristiwa Penting	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
SI-7 (8)	Perangkat Lunak, Firmware, dan Integritas Informasi | Kemampuan Audit untuk Peristiwa Penting	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (8)	Perangkat Lunak, Firmware, dan Integritas Informasi | Kemampuan Audit untuk Peristiwa Penting	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
SI-7 (8)	Perangkat Lunak, Firmware, dan Integritas Informasi | Kemampuan Audit untuk Peristiwa Penting	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (8)	Perangkat Lunak, Firmware, dan Integritas Informasi | Kemampuan Audit untuk Peristiwa Penting	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (8)	Perangkat Lunak, Firmware, dan Integritas Informasi | Kemampuan Audit untuk Peristiwa Penting	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (8)	Perangkat Lunak, Firmware, dan Integritas Informasi | Kemampuan Audit untuk Peristiwa Penting	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-7 (8)	Perangkat Lunak, Firmware, dan Integritas Informasi | Kemampuan Audit untuk Peristiwa Penting	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Manajemen dan Retensi Informasi	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Manajemen dan Retensi Informasi	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Manajemen dan Retensi Informasi	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Manajemen dan Retensi Informasi	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Manajemen dan Retensi Informasi	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Manajemen dan Retensi Informasi	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-12	Manajemen dan Retensi Informasi	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-13 (5)	Pencegahan Kegagalan yang Dapat Diprediksi | Kemampuan Failover	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-13 (5)	Pencegahan Kegagalan yang Dapat Diprediksi | Kemampuan Failover	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-13 (5)	Pencegahan Kegagalan yang Dapat Diprediksi | Kemampuan Failover	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-13 (5)	Pencegahan Kegagalan yang Dapat Diprediksi | Kemampuan Failover	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-13 (5)	Pencegahan Kegagalan yang Dapat Diprediksi | Kemampuan Failover	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-13 (5)	Pencegahan Kegagalan yang Dapat Diprediksi | Kemampuan Failover	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-13 (5)	Pencegahan Kegagalan yang Dapat Diprediksi | Kemampuan Failover	s3- version-lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihkan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).
SI-13 (5)	Pencegahan Kegagalan yang Dapat Diprediksi | Kemampuan Failover	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-13 (5)	Pencegahan Kegagalan yang Dapat Diprediksi | Kemampuan Failover	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-13 (5)	Pencegahan Kegagalan yang Dapat Diprediksi | Kemampuan Failover	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-13 (5)	Pencegahan Kegagalan yang Dapat Diprediksi | Kemampuan Failover	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-13 (5)	Pencegahan Kegagalan yang Dapat Diprediksi | Kemampuan Failover	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-13 (5)	Pencegahan Kegagalan yang Dapat Diprediksi | Kemampuan Failover	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-13 (5)	Pencegahan Kegagalan yang Dapat Diprediksi | Kemampuan Failover	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-13 (5)	Pencegahan Kegagalan yang Dapat Diprediksi | Kemampuan Failover	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-20	Mencemari	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
SI-20	Mencemari	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
SI-20	Mencemari	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk NIST 800-53 rev 5.

Praktik Terbaik Operasional untuk NIST 800 171

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini menyediakan contoh pemetaan antara aturan NIST 800-171 dan AWS Config terkelola. Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau beberapa kontrol NIST 800-171. Kontrol NIST 800-171 dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositor i data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsageUsia (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	opensearch-access-control-enabled	Pastikan kontrol akses berbutir halus diaktifkan di domain Layanan Amazon OpenSearch Anda. Kontrol akses berbutir halus menyediakan mekanisme otorisasi yang disempurnakan untuk mencapai akses yang paling tidak memiliki hak istimewa ke domain Layanan Amazon. OpenSearc h Ini memungkin kan kontrol akses berbasis peran ke domain, serta indeks, dokumen, dan keamanan tingkat lapangan, dukungan untuk dasbor OpenSearc h Layanan multi-ten ancy, dan otentikas i dasar HTTP untuk Layanan dan Kibana. OpenSearch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.1	Batasi akses sistem ke pengguna yang berwenang, proses yang bertindak atas nama pengguna yang berwenang, dan perangkat (termasuk sistem lain).	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsageUsia (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	opensearch-access-control-enabled	Pastikan kontrol akses berbutir halus diaktifkan di domain Layanan Amazon OpenSearch Anda. Kontrol akses berbutir halus menyediakan mekanisme otorisasi yang disempurnakan untuk mencapai akses yang paling tidak memiliki hak istimewa ke domain Layanan Amazon. OpenSearch Ini memungkinkan kontrol akses berbasis peran ke domain, serta indeks, dokumen, dan keamanan tingkat lapangan, dukungan untuk dasbor OpenSearch Layanan multi-tenancy, dan otentikasi dasar HTTP untuk Layanan dan Kibana. OpenSearch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.2	Batasi akses sistem ke jenis transaksi dan fungsi yang diizinkan oleh pengguna yang berwenang untuk mengeksekusi.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.
3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	opensearch-access-control-enabled	Pastikan kontrol akses berbutir halus diaktifkan di domain Layanan Amazon OpenSearch Anda. Kontrol akses berbutir halus menyediakan mekanisme otorisasi yang disempurnakan untuk mencapai akses yang paling tidak memiliki hak istimewa ke domain Layanan Amazon. OpenSearch Ini memungkinkan kontrol akses berbasis peran ke domain, serta indeks, dokumen, dan keamanan tingkat lapangan, dukungan untuk dasbor OpenSearch Layanan multi-tenancy, dan otentikasi dasar HTTP untuk Layanan dan Kibana. OpenSearch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3	Kontrol aliran CUI sesuai dengan otorisasi yang disetujui.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/ 0) akses jarak jauh dapat dikontrol ke sistem internal.
3.1.4	Pisahkan tugas individu untuk mengurangi risiko aktivitas jahat tanpa kolusi.	ec2- instance-profile-a ttached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirk an profil instans ke instans Anda dapat membantu pengelola an hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.4	Pisahkan tugas individu untuk mengurangi risiko aktivitas jahat tanpa kolusi.	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.4	Pisahkan tugas individu untuk mengurangi risiko aktivitas jahat tanpa kolusi.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.4	Pisahkan tugas individu untuk mengurangi risiko aktivitas jahat tanpa kolusi.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.4	Pisahkan tugas individu untuk mengurangi risiko aktivitas jahat tanpa kolusi.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.4	Pisahkan tugas individu untuk mengurangi risiko aktivitas jahat tanpa kolusi.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.4	Pisahkan tugas individu untuk mengurangi risiko aktivitas jahat tanpa kolusi.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.4	Pisahkan tugas individu untuk mengurangi risiko aktivitas jahat tanpa kolusi.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.4	Pisahkan tugas individu untuk mengurangi risiko aktivitas jahat tanpa kolusi.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.4	Pisahkan tugas individu untuk mengurangi risiko aktivitas jahat tanpa kolusi.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.4	Pisahkan tugas individu untuk mengurangi risiko aktivitas jahat tanpa kolusi.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsageUsia (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.4	Pisahkan tugas individu untuk mengurangi risiko aktivitas jahat tanpa kolusi.	opensearch-access-control-enabled	Pastikan kontrol akses berbutir halus diaktifkan di domain Layanan Amazon OpenSearch Anda. Kontrol akses berbutir halus menyediakan mekanisme otorisasi yang disempurnakan untuk mencapai akses yang paling tidak memiliki hak istimewa ke domain Layanan Amazon. OpenSearch Ini memungkinkan kontrol akses berbasis peran ke domain, serta indeks, dokumen, dan keamanan tingkat lapangan, dukungan untuk dasbor OpenSearch Layanan multi-tenancy, dan otentikasi dasar HTTP untuk Layanan dan Kibana. OpenSearch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.4	Pisahkan tugas individu untuk mengurangi risiko aktivitas jahat tanpa kolusi.	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs
3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	ecs-containers-nonprivileged	Untuk membantu menerapkan prinsip hak istimewa paling rendah, definisi tugas Amazon Elastic Container Service (Amazon ECS) seharusnya tidak mengaktifkan hak istimewa yang ditinggikan. Ketika parameter ini benar, wadah diberikan hak istimewa yang ditinggikan pada instance wadah host (mirip dengan pengguna root).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	ecs-containers-readonly-access	Mengaktifkan akses baca saja ke wadah Amazon Elastic Container Service (ECS) dapat membantu mematuhi prinsip hak istimewa yang paling rendah. Opsi ini dapat mengurangi vektor serangan karena sistem file instance container tidak dapat dimodifikasi kecuali jika memiliki izin baca-tulis eksplisit.
3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	ecs-task-definition-nonroot-pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan bahwa pengguna non-root ditunjuk untuk mengakses definisi tugas Amazon Elastic Container Service (Amazon ECS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	efs-access-point-enforce-identitas pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan penegakan pengguna diaktifkan untuk Amazon Elastic File System (Amazon EFS) Anda. Saat diaktifkan, Amazon EFS mengganti kan pengguna dan grup klien NFS IDs dengan identitas yang dikonfigurasi pada titik akses untuk semua operasi sistem file dan hanya memberika n akses ke identitas pengguna yang diberlakukan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsageUsia (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	opensearch-access-control-enabled	Pastikan kontrol akses berbutir halus diaktifkan di domain Layanan Amazon OpenSearch Anda. Kontrol akses berbutir halus menyediakan mekanisme otorisasi yang disempurnakan untuk mencapai akses yang paling tidak memiliki hak istimewa ke domain Layanan Amazon. OpenSearc h Ini memungkin kan kontrol akses berbasis peran ke domain, serta indeks, dokumen, dan keamanan tingkat lapangan, dukungan untuk dasbor OpenSearc h Layanan multi-ten ancy, dan otentikas i dasar HTTP untuk Layanan dan Kibana. OpenSearch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.5	Gunakan prinsip hak istimewa terkecil, termasuk untuk fungsi keamanan tertentu dan akun istimewa.	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.6	Gunakan akun atau peran yang tidak memiliki hak istimewa saat mengakses fungsi non-keamanan.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.
3.1.7	Mencegah pengguna yang tidak memiliki hak istimewa untuk menjalankan fungsi istimewa dan mengaudit pelaksana an fungsi tersebut.	iam-policy-no-stat ements-with-full-a ccess	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.7	Mencegah pengguna yang tidak memiliki hak istimewa untuk menjalankan fungsi istimewa dan mengaudit pelaksana an fungsi tersebut.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.7	Mencegah pengguna yang tidak memiliki hak istimewa untuk menjalankan fungsi istimewa dan mengaudit pelaksana an fungsi tersebut.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.7	Mencegah pengguna yang tidak memiliki hak istimewa untuk menjalankan fungsi istimewa dan mengaudit pelaksana an fungsi tersebut.	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.7	Mencegah pengguna yang tidak memiliki hak istimewa untuk menjalankan fungsi istimewa dan mengaudit pelaksana an fungsi tersebut.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.7	Mencegah pengguna yang tidak memiliki hak istimewa untuk menjalankan fungsi istimewa dan mengaudit pelaksanaan fungsi tersebut.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.7	Mencegah pengguna yang tidak memiliki hak istimewa untuk menjalankan fungsi istimewa dan mengaudit pelaksanaan fungsi tersebut.	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs
3.1.12	Pantau dan kendalikan sesi akses jarak jauh.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.12	Pantau dan kendalikan sesi akses jarak jauh.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.12	Pantau dan kendalikan sesi akses jarak jauh.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.12	Pantau dan kendalika n sesi akses jarak jauh.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.12	Pantau dan kendalikan sesi akses jarak jauh.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
3.1.12	Pantau dan kendalikan sesi akses jarak jauh.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.12	Pantau dan kendalikan sesi akses jarak jauh.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
3.1.12	Pantau dan kendalikan sesi akses jarak jauh.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.12	Pantau dan kendalikan sesi akses jarak jauh.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.12	Pantau dan kendalikan sesi akses jarak jauh.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.12	Pantau dan kendalikan sesi akses jarak jauh.	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.12	Pantau dan kendalika n sesi akses jarak jauh.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediak an metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinc i untuk permintaa n yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.12	Pantau dan kendalika n sesi akses jarak jauh.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
3.1.13	Gunakan mekanisme kriptografi untuk melindungi kerahasia an sesi akses jarak jauh.	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.13	Gunakan mekanisme kriptografi untuk melindungi kerahasia an sesi akses jarak jauh.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
3.1.13	Gunakan mekanisme kriptografi untuk melindungi kerahasia an sesi akses jarak jauh.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.13	Gunakan mekanisme kriptografi untuk melindungi kerahasia an sesi akses jarak jauh.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
3.1.13	Gunakan mekanisme kriptografi untuk melindungi kerahasia an sesi akses jarak jauh.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.13	Gunakan mekanisme kriptografi untuk melindungi kerahasiaan sesi akses jarak jauh.	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
3.1.13	Gunakan mekanisme kriptografi untuk melindungi kerahasiaan sesi akses jarak jauh.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.13	Gunakan mekanisme kriptografi untuk melindungi kerahasiaan sesi akses jarak jauh.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
3.1.14	Rutekan akses jarak jauh dari titik kontrol akses terkelola.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.14	Rutekan akses jarak jauh dari titik kontrol akses terkelola.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.14	Rutekan akses jarak jauh dari titik kontrol akses terkelola.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
3.1.14	Rutekan akses jarak jauh dari titik kontrol akses terkelola.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.14	Rutekan akses jarak jauh dari titik kontrol akses terkelola.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.1.14	Rutekan akses jarak jauh dari titik kontrol akses terkelola.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.1.14	Rutekan akses jarak jauh dari titik kontrol akses terkelola.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.14	Rutekan akses jarak jauh dari titik kontrol akses terkelola.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
3.1.14	Rutekan akses jarak jauh dari titik kontrol akses terkelola.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.14	Rutekan akses jarak jauh dari titik kontrol akses terkelola.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.14	Rutekan akses jarak jauh dari titik kontrol akses terkelola.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
3.1.14	Rutekan akses jarak jauh dari titik kontrol akses terkelola.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.14	Rutekan akses jarak jauh dari titik kontrol akses terkelola.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.14	Rutekan akses jarak jauh dari titik kontrol akses terkelola.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.14	Rutekan akses jarak jauh dari titik kontrol akses terkelola.	opensearch-access-control-enabled	Pastikan kontrol akses berbutir halus diaktifkan di domain Layanan Amazon OpenSearch Anda. Kontrol akses berbutir halus menyediakan mekanisme otorisasi yang disempurnakan untuk mencapai akses yang paling tidak memiliki hak istimewa ke domain Layanan Amazon. OpenSearch Ini memungkinkan kontrol akses berbasis peran ke domain, serta indeks, dokumen, dan keamanan tingkat lapangan, dukungan untuk dasbor OpenSearch Layanan multi-tenancy, dan otentikasi dasar HTTP untuk Layanan dan Kibana. OpenSearch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.14	Rutekan akses jarak jauh dari titik kontrol akses terkelola.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.14	Rutekan akses jarak jauh dari titik kontrol akses terkelola.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
3.1.14	Rutekan akses jarak jauh dari titik kontrol akses terkelola.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.14	Rutekan akses jarak jauh dari titik kontrol akses terkelola.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.14	Rutekan akses jarak jauh dari titik kontrol akses terkelola.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.14	Rutekan akses jarak jauh dari titik kontrol akses terkelola.	s3- account-level-publ ic-access -blok-per iodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.14	Rutekan akses jarak jauh dari titik kontrol akses terkelola.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
3.1.14	Rutekan akses jarak jauh dari titik kontrol akses terkelola.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.14	Rutekan akses jarak jauh dari titik kontrol akses terkelola.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.14	Rutekan akses jarak jauh dari titik kontrol akses terkelola.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.14	Rutekan akses jarak jauh dari titik kontrol akses terkelola.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem eksternal.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem eksternal.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem eksternal.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem eksternal.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem eksternal.	opensearch-access-control-enabled	Pastikan kontrol akses berbutir halus diaktifkan di domain Layanan Amazon OpenSearch Anda. Kontrol akses berbutir halus menyediakan mekanisme otorisasi yang disempurnakan untuk mencapai akses yang paling tidak memiliki hak istimewa ke domain Layanan Amazon. OpenSearch Ini memungkinkan kontrol akses berbasis peran ke domain, serta indeks, dokumen, dan keamanan tingkat lapangan, dukungan untuk dasbor OpenSearch Layanan multi-tenancy, dan otentikasi dasar HTTP untuk Layanan dan Kibana. OpenSearch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem eksternal.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem eksternal.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem eksternal.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem eksternal.	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem eksternal.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.20	Verifikasi dan kendali/batasi koneksi ke dan penggunaan sistem eksternal.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1	Membuat dan menyimpan catatan audit sistem sejauh yang diperlukan untuk memungkin kan pemantauan, analisis, investiga si, dan pelaporan aktivitas sistem yang melanggar hukum, tidak sah, atau tidak pantas.	cw-loggroup-retent ion-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonst ruksi dan mengident ifikasi peristiwa yang berpotensi berbahaya.
3.3.1	Membuat dan menyimpan catatan audit sistem sejauh yang diperlukan untuk memungkin kan pemantauan, analisis, investiga si, dan pelaporan aktivitas sistem yang melanggar hukum, tidak sah, atau tidak pantas.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1	Membuat dan menyimpan catatan audit sistem sejauh yang diperlukan untuk memungkin kan pemantauan, analisis, investiga si, dan pelaporan aktivitas sistem yang melanggar hukum, tidak sah, atau tidak pantas.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1	Membuat dan menyimpan catatan audit sistem sejauh yang diperlukan untuk memungkin kan pemantauan, analisis, investiga si, dan pelaporan aktivitas sistem yang melanggar hukum, tidak sah, atau tidak pantas.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1	Membuat dan menyimpan catatan audit sistem sejauh yang diperlukan untuk memungkin kan pemantauan, analisis, investiga si, dan pelaporan aktivitas sistem yang melanggar hukum, tidak sah, atau tidak pantas.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1	Membuat dan menyimpan catatan audit sistem sejauh yang diperlukan untuk memungkin kan pemantauan, analisis, investiga si, dan pelaporan aktivitas sistem yang melanggar hukum, tidak sah, atau tidak pantas.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1	Membuat dan menyimpan catatan audit sistem sejauh yang diperlukan untuk memungkin kan pemantauan, analisis, investiga si, dan pelaporan aktivitas sistem yang melanggar hukum, tidak sah, atau tidak pantas.	wafv2-logging-diak tifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatata n AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1	Membuat dan menyimpan catatan audit sistem sejauh yang diperlukan untuk memungkin kan pemantauan, analisis, investiga si, dan pelaporan aktivitas sistem yang melanggar hukum, tidak sah, atau tidak pantas.	api-gw-execution-l ogging-diaktifkan	Pencatatan API Gateway menampilk an tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
3.3.1	Membuat dan menyimpan catatan audit sistem sejauh yang diperlukan untuk memungkin kan pemantauan, analisis, investiga si, dan pelaporan aktivitas sistem yang melanggar hukum, tidak sah, atau tidak pantas.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1	Membuat dan menyimpan catatan audit sistem sejauh yang diperlukan untuk memungkin kan pemantauan, analisis, investiga si, dan pelaporan aktivitas sistem yang melanggar hukum, tidak sah, atau tidak pantas.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
3.3.1	Membuat dan menyimpan catatan audit sistem sejauh yang diperlukan untuk memungkin kan pemantauan, analisis, investiga si, dan pelaporan aktivitas sistem yang melanggar hukum, tidak sah, atau tidak pantas.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteks i aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1	Membuat dan menyimpan catatan audit sistem sejauh yang diperlukan untuk memungkin kan pemantauan, analisis, investiga si, dan pelaporan aktivitas sistem yang melanggar hukum, tidak sah, atau tidak pantas.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1	Membuat dan menyimpan catatan audit sistem sejauh yang diperlukan untuk memungkin kan pemantauan, analisis, investiga si, dan pelaporan aktivitas sistem yang melanggar hukum, tidak sah, atau tidak pantas.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1	Membuat dan menyimpan catatan audit sistem sejauh yang diperlukan untuk memungkin kan pemantauan, analisis, investiga si, dan pelaporan aktivitas sistem yang melanggar hukum, tidak sah, atau tidak pantas.	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1	Membuat dan menyimpan catatan audit sistem sejauh yang diperlukan untuk memungkin kan pemantauan, analisis, investiga si, dan pelaporan aktivitas sistem yang melanggar hukum, tidak sah, atau tidak pantas.	redshift-cluster-c onfiguration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastika n bahwa konfigura si yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberika n informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapka n untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1	Membuat dan menyimpan catatan audit sistem sejauh yang diperlukan untuk memungkin kan pemantauan, analisis, investiga si, dan pelaporan aktivitas sistem yang melanggar hukum, tidak sah, atau tidak pantas.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediak an metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinc i untuk permintaa n yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1	Membuat dan menyimpan catatan audit sistem sejauh yang diperlukan untuk memungkin kan pemantauan, analisis, investiga si, dan pelaporan aktivitas sistem yang melanggar hukum, tidak sah, atau tidak pantas.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.2	Pastikan bahwa tindakan pengguna sistem individu dapat ditelusuri secara unik ke pengguna tersebut sehingga mereka dapat bertanggung jawab atas tindakan mereka.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.2	Pastikan bahwa tindakan pengguna sistem individu dapat ditelusuri secara unik ke pengguna tersebut sehingga mereka dapat bertanggung jawab atas tindakan mereka.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
3.3.2	Pastikan bahwa tindakan pengguna sistem individu dapat ditelusuri secara unik ke pengguna tersebut sehingga mereka dapat bertanggung jawab atas tindakan mereka.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.2	Pastikan bahwa tindakan pengguna sistem individu dapat ditelusuri secara unik ke pengguna tersebut sehingga mereka dapat bertanggung jawab atas tindakan mereka.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
3.3.2	Pastikan bahwa tindakan pengguna sistem individu dapat ditelusuri secara unik ke pengguna tersebut sehingga mereka dapat bertanggung jawab atas tindakan mereka.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.2	Pastikan bahwa tindakan pengguna sistem individu dapat ditelusuri secara unik ke pengguna tersebut sehingga mereka dapat bertanggung jawab atas tindakan mereka.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.2	Pastikan bahwa tindakan pengguna sistem individu dapat ditelusuri secara unik ke pengguna tersebut sehingga mereka dapat bertanggung jawab atas tindakan mereka.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.2	Pastikan bahwa tindakan pengguna sistem individu dapat ditelusuri secara unik ke pengguna tersebut sehingga mereka dapat bertanggung jawab atas tindakan mereka.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.4	Peringatan jika terjadi kegagalan proses audit.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.4	Peringatan jika terjadi kegagalan proses audit.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.5	Mengkorelasikan tinjauan audit, analisis, dan proses pelaporan untuk investigasi dan respons terhadap indikasi aktivitas yang tidak pantas, mencurigakan, atau tidak biasa.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.5	Mengkorelasikan tinjauan audit, analisis, dan proses pelaporan untuk investigasi dan respons terhadap indikasi aktivitas yang tidak pantas, mencurigakan, atau tidak biasa.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
3.3.8	Melindungi informasi audit dan alat audit dari akses, modifikasi, dan penghapusan yang tidak sah.	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.8	Melindungi informasi audit dan alat audit dari akses, modifikasi, dan penghapusan yang tidak sah.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.8	Melindungi informasi audit dan alat audit dari akses, modifikasi, dan penghapusan yang tidak sah.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.8	Melindungi informasi audit dan alat audit dari akses, modifikasi, dan penghapusan yang tidak sah.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.8	Melindungi informasi audit dan alat audit dari akses, modifikasi, dan penghapusan yang tidak sah.	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs
3.3.8	Melindungi informasi audit dan alat audit dari akses, modifikasi, dan penghapusan yang tidak sah.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.8	Melindungi informasi audit dan alat audit dari akses, modifikasi, dan penghapusan yang tidak sah.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
3.3.8	Melindungi informasi audit dan alat audit dari akses, modifikasi, dan penghapusan yang tidak sah.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.8	Melindungi informasi audit dan alat audit dari akses, modifikasi, dan penghapusan yang tidak sah.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.1	Menetapkan dan memelihara konfigurasi dasar dan inventaris sistem organisasi (termasuk perangkat keras, perangkat lunak, firmware, dan dokumentasi) di seluruh siklus hidup pengembangan sistem masing-masing.	ec2- security-group-attached-to -eni-periodik	Aturan ini memastikan grup keamanan dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) atau ke ENI. Aturan ini membantu memantau kelompok keamanan yang tidak digunakan dalam inventaris dan pengelolaan lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.1	Menetapkan dan memelihara konfigurasi dasar dan inventaris sistem organisasi (termasuk perangkat keras, perangkat lunak, firmware, dan dokumentasi) di seluruh siklus hidup pengembangan sistem masing-masing.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.1	Menetapkan dan memelihara konfigurasi dasar dan inventaris sistem organisasi (termasuk perangkat keras, perangkat lunak, firmware, dan dokumentasi) di seluruh siklus hidup pengembangan sistem masing-masing.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.1	Menetapkan dan memelihara konfigurasi dasar dan inventaris sistem organisasi (termasuk perangkat keras, perangkat lunak, firmware, dan dokumentasi) di seluruh siklus hidup pengembangan sistem masing-masing.	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.
3.4.1	Menetapkan dan memelihara konfigurasi dasar dan inventaris sistem organisasi (termasuk perangkat keras, perangkat lunak, firmware, dan dokumentasi) di seluruh siklus hidup pengembangan sistem masing-masing.	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.1	Menetapkan dan memelihara konfigurasi dasar dan inventaris sistem organisasi (termasuk perangkat keras, perangkat lunak, firmware, dan dokumentasi) di seluruh siklus hidup pengembangan sistem masing-masing.	terlampir eip	Aturan ini memastikan Elastic IPs dialokasikan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan. Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.
3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfigurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfigurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfigurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfigurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfigurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfigurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfigurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.
3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfigurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	opensearch-access-control-enabled	Pastikan kontrol akses berbutir halus diaktifkan di domain Layanan Amazon OpenSearch Anda. Kontrol akses berbutir halus menyediakan mekanisme otorisasi yang disempurnakan untuk mencapai akses yang paling tidak memiliki hak istimewa ke domain Layanan Amazon. OpenSearc h Ini memungkin kan kontrol akses berbasis peran ke domain, serta indeks, dokumen, dan keamanan tingkat lapangan, dukungan untuk dasbor OpenSearc h Layanan multi-ten ancy, dan otentikas i dasar HTTP untuk Layanan dan Kibana. OpenSearch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfigurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfi gurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.6	Gunakan prinsip fungsionalitas terkecil dengan mengkonfigurasi sistem organisasi untuk hanya menyediakan kemampuan penting.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.7	Membatasi, menonaktifkan, dan mencegah penggunaan nonesensial, fungsi, port, protokol, atau layanan.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.7	Membatasi, menonaktifkan, dan mencegah penggunaan nonesensial, fungsi, port, protokol, atau layanan.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.7	Membatasi, menonaktifkan, dan mencegah penggunaan nonesensial, fungsi, port, protokol, atau layanan.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.7	Membatasi, menonaktifkan, dan mencegah penggunaan nonesensial, fungsi, port, protokol, atau layanan.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.9	Kontrol dan pantau perangkat lunak yang diinstal pengguna.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.9	Kontrol dan pantau perangkat lunak yang diinstal pengguna.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.2	Mengautentikasi (atau memverifi kasi) identitas pengguna, proses, atau perangkat tersebut, sebagai prasyarat untuk memungkinkan akses ke sistem organisasi.	efs-access-point-enforce-identitas pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan penegakan pengguna diaktifkan untuk Amazon Elastic File System (Amazon EFS) Anda. Saat diaktifkan, Amazon EFS mengganti kan pengguna dan grup klien NFS IDs dengan identitas yang dikonfigurasi pada titik akses untuk semua operasi sistem file dan hanya memberika n akses ke identitas pengguna yang diberlakukan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.2	Mengautentikasi (atau memverifi kasi) identitas pengguna, proses, atau perangkat tersebut, sebagai prasyarat untuk memungkinkan akses ke sistem organisasi.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastika n otentikasi multi-fak tor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindun gan ekstra di atas kredensi masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.2	Mengautentikasi (atau memverifi kasi) identitas pengguna, proses, atau perangkat tersebut, sebagai prasyarat untuk memungkinkan akses ke sistem organisasi.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredensi masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.3	Gunakan otentikasi multifaktor untuk akses lokal dan jaringan ke akun istimewa dan untuk akses jaringan ke akun yang tidak memiliki hak istimewa.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.3	Gunakan otentikasi multifaktor untuk akses lokal dan jaringan ke akun istimewa dan untuk akses jaringan ke akun yang tidak memiliki hak istimewa.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredensi masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.3	Gunakan otentikasi multifaktor untuk akses lokal dan jaringan ke akun istimewa dan untuk akses jaringan ke akun yang tidak memiliki hak istimewa.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.3	Gunakan otentikasi multifaktor untuk akses lokal dan jaringan ke akun istimewa dan untuk akses jaringan ke akun yang tidak memiliki hak istimewa.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.5	Mencegah penggunaan kembali pengidentifikasi untuk periode tertentu.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.6	Nonaktifkan pengidentifikasi setelah periode tidak aktif yang ditentukan.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsageUsia (Config Default: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.7	Terapkan kompleksitas kata sandi minimum dan perubahan karakter saat kata sandi baru dibuat.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.8	Melarang penggunaan kembali kata sandi untuk sejumlah generasi tertentu.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.10	Simpan dan kirimkan hanya kata sandi yang dilindungi secara kriptografi.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.1	Menetapkan kemampuan penanganan insiden operasional untuk sistem organisasi yang mencakup persiapan, deteksi, analisis, penahanan, pemulihan, dan aktivitas respons pengguna.	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan: rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.1	Menetapkan kemampuan penanganan insiden operasional untuk sistem organisas i yang mencakup persiapan, deteksi, analisis, penahanan , pemulihan, dan aktivitas respons pengguna.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.1	Menetapkan kemampuan penanganan insiden operasional untuk sistem organisasi yang mencakup persiapan, deteksi, analisis, penahanan, pemulihan, dan aktivitas respons pengguna.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.1	Menetapkan kemampuan penanganan insiden operasional untuk sistem organisas i yang mencakup persiapan, deteksi, analisis, penahanan , pemulihan, dan aktivitas respons pengguna.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.11.2	Memindai kerentanan dalam sistem organisasi dan aplikasi secara berkala dan ketika kerentanan baru yang mempengaruhi sistem diidentifikasi.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.11.2	Memindai kerentanan dalam sistem organisasi dan aplikasi secara berkala dan ketika kerentanan baru yang mempengaruhi sistem diidentifikasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.11.3	Memediasi kerentanan sesuai dengan penilaian risiko.	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositori data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigurasi ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	opensearch-access-control-enabled	Pastikan kontrol akses berbutir halus diaktifkan di domain Layanan Amazon OpenSearch Anda. Kontrol akses berbutir halus menyediakan mekanisme otorisasi yang disempurnakan untuk mencapai akses yang paling tidak memiliki hak istimewa ke domain Layanan Amazon. OpenSearch Ini memungkinkan kontrol akses berbasis peran ke domain, serta indeks, dokumen, dan keamanan tingkat lapangan, dukungan untuk dasbor OpenSearch Layanan multi-tenancy, dan otentikasi dasar HTTP untuk Layanan dan Kibana. OpenSearch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.1	Memantau, mengendalikan, dan melindungi komunikasi (yaitu, informasi yang dikirimkan atau diterima oleh sistem organisasi) pada batas-batas eksternal dan batas-batas internal utama sistem organisasi.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai sebenarnya harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild . Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredenal masuk dalam lingkungan proyek Codebuild . AWS Gunakan OAuth alih-alih token akses pribadi atau kredensyal masuk untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	opensearch-access-control-enabled	Pastikan kontrol akses berbutir halus diaktifkan di domain Layanan Amazon OpenSearch Anda. Kontrol akses berbutir halus menyediakan mekanisme otorisasi yang disempurnakan untuk mencapai akses yang paling tidak memiliki hak istimewa ke domain Layanan Amazon. OpenSearc h Ini memungkin kan kontrol akses berbasis peran ke domain, serta indeks, dokumen, dan keamanan tingkat lapangan, dukungan untuk dasbor OpenSearc h Layanan multi-ten ancy, dan otentikas i dasar HTTP untuk Layanan dan Kibana. OpenSearch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) menyediakan ketersediaan dan daya tahan yang ditingkatkan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			segera setelah failover selesai.
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.2	Menggunakan desain arsitektur, teknik pengembangan perangkat lunak, dan prinsip-prinsip rekayasa sistem yang mempromosikan keamanan informasi yang efektif dalam sistem organisasi.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.6	Tolak lalu lintas komunikasi jaringan secara default dan izinkan lalu lintas komunikasi jaringan dengan pengecualian (yaitu, tolak semua, izin dengan pengecualian).	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.6	Tolak lalu lintas komunikasi jaringan secara default dan izinkan lalu lintas komunikasi jaringan dengan pengecualian (yaitu, tolak semua, izin dengan pengecualian).	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.6	Tolak lalu lintas komunikasi jaringan secara default dan izinkan lalu lintas komunikasi jaringan dengan pengecualian (yaitu, tolak semua, izin dengan pengecualian).	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.8	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan CUI yang tidak sah selama transmisi kecuali dilindungi oleh perlindungan fisik alternatif.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
3.13.8	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan CUI yang tidak sah selama transmisi kecuali dilindungi oleh perlindungan fisik alternatif.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.8	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan CUI yang tidak sah selama transmisi kecuali dilindungi oleh perlindungan fisik alternatif.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.
3.13.8	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan CUI yang tidak sah selama transmisi kecuali dilindungi oleh perlindungan fisik alternatif.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.8	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan CUI yang tidak sah selama transmisi kecuali dilindungi oleh perlindungan fisik alternatif.	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
3.13.8	Menerapkan mekanisme kriptografi untuk mencegah pengungkapan CUI yang tidak sah selama transmisi kecuali dilindungi oleh perlindungan fisik alternatif.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.8	Menerapkan mekanisme kriptogra fi untuk mencegah pengungkapan CUI yang tidak sah selama transmisi kecuali dilindungi oleh perlindungan fisik alternatif.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
3.13.8	Menerapkan mekanisme kriptogra fi untuk mencegah pengungkapan CUI yang tidak sah selama transmisi kecuali dilindungi oleh perlindungan fisik alternatif.	s3- bucket-ssl-request s-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.10	Menetapkan dan mengelola kunci kriptografi untuk kriptografi yang digunakan dalam sistem organisasi.	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.
3.13.10	Menetapkan dan mengelola kunci kriptografi untuk kriptografi yang digunakan dalam sistem organisasi.	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.16	Lindungi kerahasiaan CUI saat istirahat.	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
3.13.16	Lindungi kerahasiaan CUI saat istirahat.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.16	Lindungi kerahasiaan CUI saat istirahat.	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
3.13.16	Lindungi kerahasiaan CUI saat istirahat.	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.16	Lindungi kerahasiaan CUI saat istirahat.	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.16	Lindungi kerahasiaan CUI saat istirahat.	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
3.13.16	Lindungi kerahasiaan CUI saat istirahat.	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.16	Lindungi kerahasiaan CUI saat istirahat.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
3.13.16	Lindungi kerahasiaan CUI saat istirahat.	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
3.13.16	Lindungi kerahasiaan CUI saat istirahat.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.16	Lindungi kerahasiaan CUI saat istirahat.	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
3.13.16	Lindungi kerahasiaan CUI saat istirahat.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.16	Lindungi kerahasiaan CUI saat istirahat.	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.
3.13.16	Lindungi kerahasiaan CUI saat istirahat.	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.16	Lindungi kerahasiaan CUI saat istirahat.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.16	Lindungi kerahasiaan CUI saat istirahat.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.16	Lindungi kerahasiaan CUI saat istirahat.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
3.13.16	Lindungi kerahasiaan CUI saat istirahat.	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.1	Identifikasi, laporkan, dan perbaiki kekurangan informasi dan sistem secara tepat waktu.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.1	Identifikasi, laporkan, dan perbaiki kekurangan informasi dan sistem secara tepat waktu.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.2	Memberikan perlindungan dari kode berbahaya di lokasi yang sesuai dalam sistem organisasi.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.2	Memberikan perlindungan dari kode berbahaya di lokasi yang sesuai dalam sistem organisasi.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.3	Pantau peringatan dan saran keamanan sistem dan ambil tindakan sebagai tanggapan.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.3	Pantau peringatan dan saran keamanan sistem dan ambil tindakan sebagai tanggapan.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
3.14.3	Pantau peringatan dan saran keamanan sistem dan ambil tindakan sebagai tanggapan.	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.3	Pantau peringatan dan saran keamanan sistem dan ambil tindakan sebagai tanggapan.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.3	Pantau peringatan dan saran keamanan sistem dan ambil tindakan sebagai tanggapan.	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.4	Perbarui mekanisme perlindungan kode berbahaya saat rilis baru tersedia.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.6	Memantau sistem organisasi, termasuk lalu lintas komunikasi masuk dan keluar, untuk mendeteksi serangan dan indikator serangan potensial.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.6	Memantau sistem organisasi, termasuk lalu lintas komunikasi masuk dan keluar, untuk mendeteksi serangan dan indikator serangan potensial.	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindunginya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.6	Memantau sistem organisasi, termasuk lalu lintas komunikasi masuk dan keluar, untuk mendeteksi serangan dan indikator serangan potensial.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.6	Memantau sistem organisasi, termasuk lalu lintas komunikasi masuk dan keluar, untuk mendeteksi serangan dan indikator serangan potensial.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.6	Memantau sistem organisasi, termasuk lalu lintas komunikasi masuk dan keluar, untuk mendeteksi serangan dan indikator serangan potensial.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.6	Memantau sistem organisasi, termasuk lalu lintas komunikasi masuk dan keluar, untuk mendeteksi serangan dan indikator serangan potensial.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
3.14.6	Memantau sistem organisasi, termasuk lalu lintas komunikasi masuk dan keluar, untuk mendeteksi serangan dan indikator serangan potensial.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.6	Memantau sistem organisasi, termasuk lalu lintas komunikasi masuk dan keluar, untuk mendeteksi serangan dan indikator serangan potensial.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
3.14.6	Memantau sistem organisasi, termasuk lalu lintas komunikasi masuk dan keluar, untuk mendeteksi serangan dan indikator serangan potensial.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.6	Memantau sistem organisasi, termasuk lalu lintas komunikasi masuk dan keluar, untuk mendeteksi serangan dan indikator serangan potensial.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.6	Memantau sistem organisasi, termasuk lalu lintas komunikasi masuk dan keluar, untuk mendeteksi serangan dan indikator serangan potensial.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.6	Memantau sistem organisasi, termasuk lalu lintas komunikasi masuk dan keluar, untuk mendeteksi serangan dan indikator serangan potensial.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDbEncrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.6	Memantau sistem organisasi, termasuk lalu lintas komunikasi masuk dan keluar, untuk mendeteksi serangan dan indikator serangan potensial.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.6	Memantau sistem organisasi, termasuk lalu lintas komunikasi masuk dan keluar, untuk mendeteksi serangan dan indikator serangan potensial.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
3.14.7	Identifikasi penggunaan sistem organisasi yang tidak sah.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.7	Identifikasi penggunaan sistem organisasi yang tidak sah.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.7	Identifikasi penggunaan sistem organisasi yang tidak sah.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.7	Identifikasi penggunaan sistem organisasi yang tidak sah.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.7	Identifikasi penggunaan sistem organisasi yang tidak sah.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
3.14.7	Identifikasi penggunaan sistem organisasi yang tidak sah.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.7	Identifikasi penggunaan sistem organisasi yang tidak sah.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
3.14.7	Identifikasi penggunaan sistem organisasi yang tidak sah.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.7	Identifikasi penggunaan sistem organisasi yang tidak sah.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.7	Identifikasi penggunaan sistem organisasi yang tidak sah.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.7	Identifikasi penggunaan sistem organisasi yang tidak sah.	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.7	Identifikasi penggunaan sistem organisasi yang tidak sah.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.7	Identifikasi penggunaan sistem organisasi yang tidak sah.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.7	Identifikasi penggunaan sistem organisasi yang tidak sah.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk NIST 800 171.

Praktik Terbaik Operasional untuk NIST 800 172

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini menyediakan contoh pemetaan antara aturan NIST 800-172 dan AWS Config terkelola. Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau beberapa kontrol NIST 800-172. Kontrol NIST 800-172 dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	alb-http-drop-invalid-Header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	domain keamanan pada sistem yang terhubung.		backend mengautentikasi permintaan yang berasal dari API Gateway.
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigurasi ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	alb-desync-mode-check	Untuk membantu melindungi aplikasi untuk kerentanan HTTP Desync, pastikan mode mitigasi HTTP Desync diaktifkan pada penyeimbang beban aplikasi Anda. Masalah HTTP Desync dapat menyebabkan penyelundupan permintaan dan membuat aplikasi Anda rentan terhadap antrian permintaan atau keracunan cache. Mode mitigasi desync adalah monitor, defensif, dan paling ketat. Defensif adalah mode default.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	clb-desync-mode-check	Untuk membantu melindungi aplikasi untuk kerentanan HTTP Desync, pastikan mode mitigasi HTTP Desync diaktifkan pada penyeimbang beban aplikasi Anda. Masalah HTTP Desync dapat menyebabkan penyelundupan permintaan dan membuat aplikasi Anda rentan terhadap antrian permintaan atau keracunan cache. Mode mitigasi desync adalah monitor, defensif, dan paling ketat. Defensif adalah mode default.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositori data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	ec2- token-hop-limit-check	Pastikan respons PUT HTTP Instance Metadata Service (IMDS) dibatasi pada instans Amazon Elastic Compute Cloud (Amazon). EC2 Dengan IMDSv2, respons PUT yang berisi token rahasia secara default tidak dapat berjalan di luar instance, karena batas hop respons Metadata diatur ke 1 (Config default). Jika nilai ini lebih besar dari 1, token dapat meninggalkan EC2 instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1.3e	Gunakan [Penugasan: solusi transfer informasi aman yang ditentukan organisasi] untuk mengontrol arus informasi antara domain keamanan pada sistem yang terhubung.	nacl-no-unrestricted-ssh-rdp	Akses ke port administrasi server jarak jauh di Daftar Kontrol Akses Jaringan Anda (NACLs), seperti port 22 (SSH) dan port 3389 (RDP), tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke sumber daya dalam VPC Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.2.1e	Memberikan pelatihan kesadaran [Penugasan: frekuensi yang ditentukan organisasi] yang berfokus pada mengenali dan menanggapi ancaman dari rekayasa sosial, aktor ancaman persisten tingkat lanjut, pelanggaran, dan perilaku mencurigakan; memperbarui pelatihan [Penugasan: frekuensi yang ditentukan organisasi] atau ketika ada perubahan signifikan terhadap ancaman.	security-awareness-program-exists (pemeriksaan proses)	Membangun dan memelihara program kesadaran keamanan untuk organisasi Anda. Program kesadaran keamanan mendidik karyawan tentang cara melindungi organisasi mereka dari berbagai pelanggaran atau insiden keamanan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.2e	Menggunakan mekanisme otomatis untuk mendeteksi komponen sistem yang salah dikonfigurasi atau tidak sah; setelah deteksi, [Seleksi (satu atau lebih): lepaskan komponen; tempatkan komponen dalam jaringan karantina atau remediasi] untuk memfasilitasi penambalan, konfigurasi ulang, atau mitigasi lainnya.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.2e	Menggunakan mekanisme otomatis untuk mendeteksi komponen sistem yang salah dikonfigurasi atau tidak sah; setelah deteksi, [Seleksi (satu atau lebih): lepaskan komponen; tempatkan komponen dalam jaringan karantina atau remediasi] untuk memfasilitasi penambalan, konfigurasi ulang, atau mitigasi lainnya.	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.2e	Menggunakan mekanisme otomatis untuk mendeteksi komponen sistem yang salah dikonfigurasi atau tidak sah; setelah deteksi, [Seleksi (satu atau lebih): lepaskan komponen; tempatkan komponen dalam jaringan karantina atau remediasi] untuk memfasilitasi penambalan, konfigurasi ulang, atau mitigasi lainnya.	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.2e	Menggunakan mekanisme otomatis untuk mendeteksi komponen sistem yang salah dikonfigurasi atau tidak sah; setelah deteksi, [Seleksi (satu atau lebih): lepaskan komponen; tempatkan komponen dalam jaringan karantina atau remediasi] untuk memfasilitasi penambalan, konfigurasi ulang, atau mitigasi lainnya.	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relational Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.3e	Gunakan alat penemuan dan manajemen otomatis untuk memelihara inventaris komponen sistem yang lengkap up-to-date, akurat, dan tersedia.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.3e	Gunakan alat penemuan dan manajemen otomatis untuk memelihara inventaris komponen sistem yang lengkap up-to-date, akurat, dan tersedia.	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.
3.4.3e	Gunakan alat penemuan dan manajemen otomatis untuk memelihara inventaris komponen sistem yang lengkap up-to-date, akurat, dan tersedia.	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4.3e	Gunakan alat penemuan dan manajemen otomatis untuk memelihara inventaris komponen sistem yang lengkap up-to-date, akurat, dan tersedia.	terlampir eip	Aturan ini memastikan Elastic yang IPs dialokasikan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan. Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.
3.4.3e	Gunakan alat penemuan dan manajemen otomatis untuk memelihara inventaris komponen sistem yang lengkap up-to-date, akurat, dan tersedia.	vpc-network-acl-unused-periksa	Aturan ini memastikan bahwa daftar kontrol akses jaringan Amazon Virtual Private Cloud (VPC) sedang digunakan. Pemantauan untuk daftar kontrol akses jaringan yang tidak digunakan dapat membantu inventaris dan pengelolaan lingkungan Anda yang akurat.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.2e	Gunakan mekanisme otomatis untuk pembuatan, perlindungan, rotasi, dan pengelolaan kata sandi untuk sistem dan komponen sistem yang tidak mendukung otentikasi multifaktor atau manajemen akun yang kompleks.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
3.5.2e	Gunakan mekanisme otomatis untuk pembuatan, perlindungan, rotasi, dan pengelolaan kata sandi untuk sistem dan komponen sistem yang tidak mendukung otentikasi multifaktor atau manajemen akun yang kompleks.	secretsmanager-rotation-enabled-check	Aturan ini memastikan AWS rahasia Secrets Manager mengaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.2e	Gunakan mekanisme otomatis untuk pembuatan, perlindungan, rotasi, dan pengelolaan kata sandi untuk sistem dan komponen sistem yang tidak mendukung otentikasi multifaktor atau manajemen akun yang kompleks.	secretsmanager-scheduled-rotation-success-periksa	Aturan ini memastikan bahwa AWS rahasia Secrets Manager telah berhasil diputar sesuai dengan jadwal rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode di mana rahasia aktif, dan berpotensi mengurangi dampak bisnis jika dikompromikan.
3.5.2e	Gunakan mekanisme otomatis untuk pembuatan, perlindungan, rotasi, dan pengelolaan kata sandi untuk sistem dan komponen sistem yang tidak mendukung otentikasi multifaktor atau manajemen akun yang kompleks.	secretsmanager-scheduled-rotation-success-periksa	Aturan ini memastikan bahwa AWS rahasia Secrets Manager telah berhasil diputar sesuai dengan jadwal rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode di mana rahasia aktif, dan berpotensi mengurangi dampak bisnis jika dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.11.1e	Mempekerjakan [Penugasan: sumber intelijen ancaman yang ditentukan organisasi] sebagai bagian dari penilaian risiko untuk memandu dan menginfor masikan pengemban gan sistem organisasi, arsitektur keamanan, pemilihan solusi keamanan, pemantauan, perburuan ancaman, dan kegiatan respons dan pemulihan.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.11.2e	Melakukan kegiatan berburu ancaman cyber [Seleksi (satu atau lebih): [Penugasan: frekuensi yang ditentuka n organisasi]; [Penugasan: acara yang ditentuka n organisasi]] untuk mencari indikator kompromi di [Penugasan: sistem yang ditentuka n organisasi] dan mendeteksi, melacak, dan menggangg u ancaman yang menghindari kontrol yang ada.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
3.11.5e	Menilai efektivitas solusi keamanan [Penugasan: frekuensi yang ditentukan organisasi] untuk mengatasi risiko yang diantisipasi terhadap sistem organisasi dan organisasi berdasark an intelijen ancaman saat ini dan akumulasi .	annual-risk-assess ment-performed (pemeriksaan proses)	Lakukan penilaian risiko tahunan pada organisasi Anda. Penilaian risiko dapat membantu dalam menentuka n kemungkinan dan dampak dari risiko dan/atau kerentana n yang diidentifikasi yang mempengaruhi suatu organisasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.4e	Mempekerjakan [Seleksi: (satu atau lebih): [Tugas: teknik isolasi fisik yang ditentukan organisasi]; [Tugas: teknik isolasi logis yang ditentukan organisasi]] dalam sistem organisasi dan komponen sistem.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.13.4e	Mempekerjakan [Seleksi: (satu atau lebih): [Tugas: teknik isolasi fisik yang ditentukan organisasi]; [Tugas: teknik isolasi logis yang ditentukan organisasi]] dalam sistem organisasi dan komponen sistem.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.4e	Mempekerjakan [Seleksi: (satu atau lebih): [Tugas: teknik isolasi fisik yang ditentukan organisasi]; [Tugas: teknik isolasi logis yang ditentukan organisasi]] dalam sistem organisasi dan komponen sistem.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
3.13.4e	Mempekerjakan [Seleksi: (satu atau lebih): [Tugas: teknik isolasi fisik yang ditentukan organisasi]; [Tugas: teknik isolasi logis yang ditentukan organisasi]] dalam sistem organisasi dan komponen sistem.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.4e	Mempekerjakan [Seleksi: (satu atau lebih): [Tugas: teknik isolasi fisik yang ditentukan organisasi]; [Tugas: teknik isolasi logis yang ditentukan organisasi]] dalam sistem organisasi dan komponen sistem.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.4e	Mempekerjakan [Seleksi: (satu atau lebih): [Tugas: teknik isolasi fisik yang ditentukan organisasi]; [Tugas: teknik isolasi logis yang ditentukan organisasi]] dalam sistem organisasi dan komponen sistem.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.4e	Mempekerjakan [Seleksi: (satu atau lebih): [Tugas: teknik isolasi fisik yang ditentukan organisasi]; [Tugas: teknik isolasi logis yang ditentukan organisasi]] dalam sistem organisasi dan komponen sistem.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.4e	Mempekerjakan [Seleksi: (satu atau lebih): [Tugas: teknik isolasi fisik yang ditentukan organisasi]; [Tugas: teknik isolasi logis yang ditentukan organisasi]] dalam sistem organisasi dan komponen sistem.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigurasi ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.4e	Mempekerjakan [Seleksi: (satu atau lebih): [Tugas: teknik isolasi fisik yang ditentukan organisasi]; [Tugas: teknik isolasi logis yang ditentukan organisasi]] dalam sistem organisasi dan komponen sistem.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
3.13.4e	Mempekerjakan [Seleksi: (satu atau lebih): [Tugas: teknik isolasi fisik yang ditentukan organisasi]; [Tugas: teknik isolasi logis yang ditentukan organisasi]] dalam sistem organisasi dan komponen sistem.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.4e	Mempekerjakan [Seleksi: (satu atau lebih): [Tugas: teknik isolasi fisik yang ditentukan organisasi]; [Tugas: teknik isolasi logis yang ditentukan organisasi]] dalam sistem organisasi dan komponen sistem.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.4e	Mempekerjakan [Seleksi: (satu atau lebih): [Tugas: teknik isolasi fisik yang ditentukan organisasi]; [Tugas: teknik isolasi logis yang ditentukan organisasi]] dalam sistem organisasi dan komponen sistem.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.4e	Mempekerjakan [Seleksi: (satu atau lebih): [Tugas: teknik isolasi fisik yang ditentukan organisasi]; [Tugas: teknik isolasi logis yang ditentukan organisasi]] dalam sistem organisasi dan komponen sistem.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
3.13.4e	Mempekerjakan [Seleksi: (satu atau lebih): [Tugas: teknik isolasi fisik yang ditentukan organisasi]; [Tugas: teknik isolasi logis yang ditentukan organisasi]] dalam sistem organisasi dan komponen sistem.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.4e	Mempekerjakan [Seleksi: (satu atau lebih): [Tugas: teknik isolasi fisik yang ditentukan organisasi]; [Tugas: teknik isolasi logis yang ditentukan organisasi]] dalam sistem organisasi dan komponen sistem.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
3.13.4e	Mempekerjakan [Seleksi: (satu atau lebih): [Tugas: teknik isolasi fisik yang ditentukan organisasi]; [Tugas: teknik isolasi logis yang ditentukan organisasi]] dalam sistem organisasi dan komponen sistem.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.4e	Mempekerjakan [Seleksi: (satu atau lebih): [Tugas: teknik isolasi fisik yang ditentukan organisasi]; [Tugas: teknik isolasi logis yang ditentukan organisasi]] dalam sistem organisasi dan komponen sistem.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.4e	Mempekerjakan [Seleksi: (satu atau lebih): [Tugas: teknik isolasi fisik yang ditentukan organisasi]; [Tugas: teknik isolasi logis yang ditentukan organisasi]] dalam sistem organisasi dan komponen sistem.	nacl-no-unrestricted-ssh-rdp	Akses ke port administrasi server jarak jauh di Daftar Kontrol Akses Jaringan Anda (NACLs), seperti port 22 (SSH) dan port 3389 (RDP), tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke sumber daya dalam VPC Anda.
3.13.4e	Mempekerjakan [Seleksi: (satu atau lebih): [Tugas: teknik isolasi fisik yang ditentukan organisasi]; [Tugas: teknik isolasi logis yang ditentukan organisasi]] dalam sistem organisasi dan komponen sistem.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.4e	Mempekerjakan [Seleksi: (satu atau lebih): [Tugas: teknik isolasi fisik yang ditentukan organisasi]; [Tugas: teknik isolasi logis yang ditentukan organisasi]] dalam sistem organisasi dan komponen sistem.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
3.13.4e	Mempekerjakan [Seleksi: (satu atau lebih): [Tugas: teknik isolasi fisik yang ditentukan organisasi]; [Tugas: teknik isolasi logis yang ditentukan organisasi]] dalam sistem organisasi dan komponen sistem.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.4e	Mempekerjakan [Seleksi: (satu atau lebih): [Tugas: teknik isolasi fisik yang ditentukan organisasi]; [Tugas: teknik isolasi logis yang ditentukan organisasi]] dalam sistem organisasi dan komponen sistem.	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositori data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.4e	Mempekerjakan [Seleksi: (satu atau lebih): [Tugas: teknik isolasi fisik yang ditentukan organisasi]; [Tugas: teknik isolasi logis yang ditentukan organisasi]] dalam sistem organisasi dan komponen sistem.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.4e	Mempekerjakan [Seleksi: (satu atau lebih): [Tugas: teknik isolasi fisik yang ditentukan organisasi]; [Tugas: teknik isolasi logis yang ditentukan organisasi]] dalam sistem organisasi dan komponen sistem.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.4e	Mempekerjakan [Seleksi: (satu atau lebih): [Tugas: teknik isolasi fisik yang ditentukan organisasi]; [Tugas: teknik isolasi logis yang ditentukan organisasi]] dalam sistem organisasi dan komponen sistem.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.4e	Mempekerjakan [Seleksi: (satu atau lebih): [Tugas: teknik isolasi fisik yang ditentukan organisasi]; [Tugas: teknik isolasi logis yang ditentukan organisasi]] dalam sistem organisasi dan komponen sistem.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.13.4e	Mempekerjakan [Seleksi: (satu atau lebih): [Tugas: teknik isolasi fisik yang ditentukan organisasi]; [Tugas: teknik isolasi logis yang ditentukan organisasi]] dalam sistem organisasi dan komponen sistem.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.1e	Verifikasi integrita s [Penugasan: perangkat lunak penting atau penting keamanan yang ditentukan organisas i] menggunakan akar mekanisme kepercayaan atau tanda tangan kriptografi.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.2e	Memantau sistem organisasi dan komponen sistem secara berkelanj utan untuk perilaku anomali atau mencurigakan.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
3.14.2e	Memantau sistem organisasi dan komponen sistem secara berkelanj utan untuk perilaku anomali atau mencurigakan.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.2e	Memantau sistem organisasi dan komponen sistem secara berkelanj utan untuk perilaku anomali atau mencurigakan.	cloudwatch-alarm-a ction-check	Amazon CloudWatc h mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasark an pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActi onRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.2e	Memantau sistem organisasi dan komponen sistem secara berkelanj utan untuk perilaku anomali atau mencurigakan.	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.2e	Memantau sistem organisasi dan komponen sistem secara berkelanj utan untuk perilaku anomali atau mencurigakan.	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.2e	Memantau sistem organisasi dan komponen sistem secara berkelanj utan untuk perilaku anomali atau mencurigakan.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.2e	Memantau sistem organisasi dan komponen sistem secara berkelanj utan untuk perilaku anomali atau mencurigakan.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.6e	Gunakan informasi indikator ancaman dan mitigasi efektif yang diperoleh dari [Penugasan: organisasi eksternal yang ditentukan organisasi] untuk memandu dan menginformasikan deteksi intrusi dan perburuan ancaman.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.7e	Verifikasi kebenaran [Penugasan: perangkat lunak, firmware, dan komponen perangkat keras yang ditentukan keamanan yang ditentukan organisasi] menggunakan [Penugasan: metode atau teknik verifikasi yang ditentukan organisasi].	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.7e	Verifikasi kebenaran [Penugasan: perangkat lunak, firmware, dan komponen perangkat keras yang ditentukan keamanan yang ditentukan organisasi] menggunakan [Penugasan: metode atau teknik verifikasi yang ditentukan organisasi].	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.7e	Verifikasi kebenaran [Penugasan: perangkat lunak, firmware, dan komponen perangkat keras yang ditentuka n keamanan yang ditentukan organisas i] menggunakan [Penugasan: metode atau teknik verifikas i yang ditentukan organisasi].	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.7e	Verifikasi kebenaran [Penugasan: perangkat lunak, firmware, dan komponen perangkat keras yang ditentuka n keamanan yang ditentukan organisas i] menggunakan [Penugasan: metode atau teknik verifikas i yang ditentukan organisasi].	ecs-fargate-latest-platform-versi	Pembaruan dan tambalan keamanan diterapkan secara otomatis untuk tugas Fargate AWS Anda. Jika ditemukan masalah keamanan yang memengaru hi versi platform AWS Fargate, AWS tambal versi platform. Untuk membantu pengelolaan tambalan tugas Amazon Elastic Container Service (ECS) yang menjalank an AWS Fargate, perbarui tugas mandiri layanan Anda untuk menggunakan versi platform terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.14.7e	Verifikasi kebenaran [Penugasan: perangkat lunak, firmware, dan komponen perangkat keras yang ditentukan keamanan yang ditentukan organisasi] menggunakan [Penugasan: metode atau teknik verifikasi yang ditentukan organisasi].	ecr-private-image-scanning-diaktifkan	Pemindaian gambar Amazon Elastic Container Repository (ECR) membantu mengidentifikasi kerentanan perangkat lunak dalam gambar kontainer Anda. Mengaktifkan pemindaian gambar pada repositori ECR menambahkan lapisan verifikasi untuk integritas dan keamanan gambar yang disimpan.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk NIST 800 172.

Praktik Terbaik Operasional untuk NIST 800 181

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini menyediakan contoh pemetaan antara aturan NIST 800 181 dan AWS Config terkelola. Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan berhubungan dengan satu atau beberapa kontrol NIST 800 181. Kontrol NIST 800 181 dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0008	Menganalisis dan merencanakan perubahan yang diantisipasi dalam persyaratan kapasitas data.	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.
T0008	Menganalisis dan merencanakan perubahan yang diantisipasi dalam persyaratan kapasitas data.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.
T0008	Menganalisis dan merencanakan perubahan yang diantisipasi dalam persyaratan kapasitas data.	dynamodb-pitr-enab led	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertah ankan cadangan dengan memastika n bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0008	Menganalisis dan merencanakan perubahan yang diantisipasi dalam persyaratan kapasitas data.	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
T0008	Menganalisis dan merencanakan perubahan yang diantisipasi dalam persyaratan kapasitas data.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0008	Menganalisis dan merencanakan perubahan yang diantisipasi dalam persyaratan kapasitas data.	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0008	Menganalisis dan merencanakan perubahan yang diantisipasi dalam persyaratan kapasitas data.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0008	Menganalisis dan merencanakan perubahan yang diantisipasi dalam persyaratan kapasitas data.	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0008	Menganalisis dan merencanakan perubahan yang diantisipasi dalam persyaratan kapasitas data.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0008	Menganalisis dan merencanakan perubahan yang diantisipasi dalam persyaratan kapasitas data.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) menyediakan ketersediaan dan daya tahan yang ditingkatkan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			segera setelah failover selesai.
T0008	Menganalisis dan merencanakan perubahan yang diantisipasi dalam persyaratan kapasitas data.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0008	Menganalisis dan merencanakan perubahan yang diantisipasi dalam persyaratan kapasitas data.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0008	Menganalisis dan merencanakan perubahan yang diantisipasi dalam persyaratan kapasitas data.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0008	Menganalisis dan merencanakan perubahan yang diantisipasi dalam persyaratan kapasitas data.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	backup-recovery-point-manual-penghapusan dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain Amazon Elasticsearch Service (Amazon ES) Anda.
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorient asi layanan untuk memenuhi persyarat an kerahasiaan, integritas, dan ketersediaan organisasi.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorient asi layanan untuk memenuhi persyarat an kerahasiaan, integritas, dan ketersediaan organisasi.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDbEncrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorient asi layanan untuk memenuhi persyarat an kerahasiaan, integritas, dan ketersediaan organisasi.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
T0017	Menerapkan prinsip-prinsip arsitektur keamanan berorientasi layanan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan organisasi.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0024	Mengumpulkan dan memelihara data yang diperlukan untuk memenuhi pelaporan keamanan siber sistem.	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.
T0042	Berkoordinasi dengan Analis Pertahanan Siber untuk mengelola dan mengelola pembaruan aturan dan tanda tangan (misalnya, sistem deteksi/perlindungan intrusi, antivirus, dan daftar hitam konten) untuk aplikasi pertahanan cyber khusus.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0047	Korelasikan data insiden untuk mengidentifikasi kerentanan tertentu dan membuat rekomendasi yang memungkinkan remediasi cepat.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0051	Tentukan tingkat ketersediaan sistem yang sesuai berdasarkan fungsi sistem kritis dan pastikan bahwa persyaratan sistem mengidentifikasi pemulihan bencana yang tepat dan kelangsungan persyaratan operasi untuk memasukkan kegagalan yang sesuai. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0051	Tentukan tingkat ketersediaan sistem yang sesuai berdasarkan fungsi sistem kritis dan pastikan bahwa persyaratan sistem mengidentifikasi pemulihan bencana yang tepat dan kelangsungan persyaratan operasi untuk memasukkan kegagalan yang sesuai. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	backup-recovery-point-manual-penghapusan dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0051	Tentukan tingkat ketersediaan sistem yang sesuai berdasarkan fungsi sistem kritis dan pastikan bahwa persyaratan sistem mengidentifikasi pemulihan bencana yang tepat dan kelangsungan persyaratan operasi untuk memasukkan kegagalan yang sesuai. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0051	Tentukan tingkat ketersediaan sistem yang sesuai berdasarkan fungsi sistem kritis dan pastikan bahwa persyaratan sistem mengidentifikasi pemulihan bencana yang tepat dan kelangsungan persyaratan operasi untuk memasukkan kegagalan yang sesuai. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0051	Tentukan tingkat ketersediaan sistem yang sesuai berdasarkan fungsi sistem kritis dan pastikan bahwa persyaratan sistem mengidentifikasi pemulihan bencana yang tepat dan kelangsungan persyaratan operasi untuk memasukkan kegagalan yang sesuai. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0051	Tentukan tingkat ketersediaan sistem yang sesuai berdasarkan fungsi sistem kritis dan pastikan bahwa persyaratan sistem mengidentifikasi pemulihan bencana yang tepat dan kelangsungan persyaratan operasi untuk memasukkan kegagalan yang sesuai. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0051	Tentukan tingkat ketersediaan sistem yang sesuai berdasarkan fungsi sistem kritis dan pastikan bahwa persyaratan sistem mengidentifikasi pemulihan bencana yang tepat dan kelangsungan persyaratan operasi untuk memasukkan kegagalan yang sesuai. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
T0051	Tentukan tingkat ketersediaan sistem yang sesuai berdasarkan fungsi sistem kritis dan pastikan bahwa persyaratan sistem mengidentifikasi pemulihan bencana yang tepat dan kelangsungan persyaratan operasi untuk memasukkan kegagalan yang sesuai. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0051	Tentukan tingkat ketersediaan sistem yang sesuai berdasarkan fungsi sistem kritis dan pastikan bahwa persyaratan sistem mengidentifikasi pemulihan bencana yang tepat dan kelangsungan persyaratan operasi untuk memasukkan kegagalan yang sesuai. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0051	Tentukan tingkat ketersediaan sistem yang sesuai berdasarkan fungsi sistem kritis dan pastikan bahwa persyaratan sistem mengidentifikasi pemulihan bencana yang tepat dan kelangsungan persyaratan operasi untuk memasukkan kegagalan yang sesuai. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0051	Tentukan tingkat ketersediaan sistem yang sesuai berdasarkan fungsi sistem kritis dan pastikan bahwa persyaratan sistem mengidentifikasi pemulihan bencana yang tepat dan kelangsungan persyaratan operasi untuk memasukkan kegagalan yang sesuai. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0051	Tentukan tingkat ketersediaan sistem yang sesuai berdasarkan fungsi sistem kritis dan pastikan bahwa persyaratan sistem mengidentifikasi pemulihan bencana yang tepat dan kelangsungan persyaratan operasi untuk memasukkan kegagalan yang sesuai. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0051	Tentukan tingkat ketersediaan sistem yang sesuai berdasarkan fungsi sistem kritis dan pastikan bahwa persyaratan sistem mengidentifikasi pemulihan bencana yang tepat dan kelangsungan persyaratan operasi untuk memasukkan kegagalan yang sesuai. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0051	Tentukan tingkat ketersediaan sistem yang sesuai berdasarkan fungsi sistem kritis dan pastikan bahwa persyaratan sistem mengidentifikasi pemulihan bencana yang tepat dan kelangsungan persyaratan operasi untuk memasukkan kegagalan yang sesuai. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relational Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0051	Tentukan tingkat ketersediaan sistem yang sesuai berdasarkan fungsi sistem kritis dan pastikan bahwa persyaratan sistem mengidentifikasi pemulihan bencana yang tepat dan kelangsungan persyaratan operasi untuk memasukkan kegagalan yang sesuai. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0051	Tentukan tingkat ketersediaan sistem yang sesuai berdasarkan fungsi sistem kritis dan pastikan bahwa persyaratan sistem mengidentifikasi pemulihan bencana yang tepat dan kelangsungan persyaratan operasi untuk memasukkan kegagalan yang sesuai. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0051	Tentukan tingkat ketersediaan sistem yang sesuai berdasarkan fungsi sistem kritis dan pastikan bahwa persyaratan sistem mengidentifikasi pemulihan bencana yang tepat dan kelangsungan persyaratan operasi untuk memasukkan kegagalan yang sesuai. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0051	Tentukan tingkat ketersediaan sistem yang sesuai berdasarkan fungsi sistem kritis dan pastikan bahwa persyaratan sistem mengidentifikasi pemulihan bencana yang tepat dan kelangsungan persyaratan operasi untuk memasukka n kegagalan yang sesuai. over/alternate site requirements, backup requireme nts, and material supportability requirements for system recover/r estoration	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0051	Tentukan tingkat ketersediaan sistem yang sesuai berdasarkan fungsi sistem kritis dan pastikan bahwa persyaratan sistem mengidentifikasi pemulihan bencana yang tepat dan kelangsungan persyaratan operasi untuk memasukkan kegagalan yang sesuai. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0051	Tentukan tingkat ketersediaan sistem yang sesuai berdasarkan fungsi sistem kritis dan pastikan bahwa persyaratan sistem mengidentifikasi pemulihan bencana yang tepat dan kelangsungan persyaratan operasi untuk memasukkan kegagalan yang sesuai. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0051	Tentukan tingkat ketersediaan sistem yang sesuai berdasarkan fungsi sistem kritis dan pastikan bahwa persyaratan sistem mengidentifikasi pemulihan bencana yang tepat dan kelangsungan persyaratan operasi untuk memasukkan kegagalan yang sesuai. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0065	Mengembangkan dan menerapkan prosedur pencadangan dan pemulihan jaringan.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0065	Mengembangkan dan menerapkan prosedur pencadangan dan pemulihan jaringan.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
T0065	Mengembangkan dan menerapkan prosedur pencadangan dan pemulihan jaringan.	backup-recovery-point-manual-penghapusan dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0065	Mengembangkan dan menerapkan prosedur pencadangan dan pemulihan jaringan.	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0065	Mengembangkan dan menerapkan prosedur pencadangan dan pemulihan jaringan.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0065	Mengembangkan dan menerapkan prosedur pencadangan dan pemulihan jaringan.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0065	Mengembangkan dan menerapkan prosedur pencadangan dan pemulihan jaringan.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0065	Mengembangkan dan menerapkan prosedur pencadangan dan pemulihan jaringan.	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0065	Mengembangkan dan menerapkan prosedur pencadangan dan pemulihan jaringan.	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0065	Mengembangkan dan menerapkan prosedur pencadangan dan pemulihan jaringan.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0065	Mengembangkan dan menerapkan prosedur pencadangan dan pemulihan jaringan.	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0065	Mengembangkan dan menerapkan prosedur pencadangan dan pemulihan jaringan.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0065	Mengembangkan dan menerapkan prosedur pencadangan dan pemulihan jaringan.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0065	Mengembangkan dan menerapkan prosedur pencadangan dan pemulihan jaringan.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0065	Mengembangkan dan menerapkan prosedur pencadangan dan pemulihan jaringan.	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0065	Mengembangkan dan menerapkan prosedur pencadangan dan pemulihan jaringan.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0065	Mengembangkan dan menerapkan prosedur pencadangan dan pemulihan jaringan.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0065	Mengembangkan dan menerapkan prosedur pencadangan dan pemulihan jaringan.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0065	Mengembangkan dan menerapkan prosedur pencadangan dan pemulihan jaringan.	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0065	Mengembangkan dan menerapkan prosedur pencadangan dan pemulihan jaringan.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0065	Mengembangkan dan menerapkan prosedur pencadangan dan pemulihan jaringan.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0070	Mengembangkan rencana Pemulihan Bencana dan Kontinuitas Operasi untuk sistem yang sedang dikembang kan dan memastika n pengujian sebelum sistem memasuki lingkungan produksi.	backup-plan-min-fr equency-and-min-re tention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkin kan Anda untuk mengatur parameter requiredFrequencyV alue (Config default: 1), (requiredR etentionDaysConfig default: 35) dan (requiredFrequencyU nit Config default: days). Nilai aktual harus mencerminkan persyaratan organisas i Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0070	Mengembangkan rencana Pemulihan Bencana dan Kontinuitas Operasi untuk sistem yang sedang dikembang kan dan memastika n pengujian sebelum sistem memasuki lingkungan produksi.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
T0070	Mengembangkan rencana Pemulihan Bencana dan Kontinuitas Operasi untuk sistem yang sedang dikembang kan dan memastika n pengujian sebelum sistem memasuki lingkungan produksi.	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapus an titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapus an titik pemulihan dapat membantu mencegah penghapus an yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0070	Mengembangkan rencana Pemulihan Bencana dan Kontinuitas Operasi untuk sistem yang sedang dikembang kan dan memastika n pengujian sebelum sistem memasuki lingkungan produksi.	dynamodb-in-backup-plan	Untuk membantu proses pencadang an data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0070	Mengembangkan rencana Pemulihan Bencana dan Kontinuitas Operasi untuk sistem yang sedang dikembang kan dan memastika n pengujian sebelum sistem memasuki lingkungan produksi.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0070	Mengembangkan rencana Pemulihan Bencana dan Kontinuitas Operasi untuk sistem yang sedang dikembang kan dan memastika n pengujian sebelum sistem memasuki lingkungan produksi.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0070	Mengembangkan rencana Pemulihan Bencana dan Kontinuitas Operasi untuk sistem yang sedang dikembang kan dan memastika n pengujian sebelum sistem memasuki lingkungan produksi.	efs-in-backup-plan	Untuk membantu proses pencadang an data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0070	Mengembangkan rencana Pemulihan Bencana dan Kontinuitas Operasi untuk sistem yang sedang dikembang kan dan memastika n pengujian sebelum sistem memasuki lingkungan produksi.	elb-cross-zone-loa d-menyeimbangkan diaktifkan	Aktifkan penyeimba ngan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimba ngan beban lintas zona mengurang i kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkat kan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0070	Mengembangkan rencana Pemulihan Bencana dan Kontinuitas Operasi untuk sistem yang sedang dikembang kan dan memastika n pengujian sebelum sistem memasuki lingkungan produksi.	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relationa l Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindun gan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersedi aan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0070	Mengembangkan rencana Pemulihan Bencana dan Kontinuitas Operasi untuk sistem yang sedang dikembang kan dan memastika n pengujian sebelum sistem memasuki lingkungan produksi.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0070	Mengembangkan rencana Pemulihan Bencana dan Kontinuitas Operasi untuk sistem yang sedang dikembang kan dan memastika n pengujian sebelum sistem memasuki lingkungan produksi.	redshift-backup-en abled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifka n untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0070	Mengembangkan rencana Pemulihan Bencana dan Kontinuitas Operasi untuk sistem yang sedang dikembang kan dan memastika n pengujian sebelum sistem memasuki lingkungan produksi.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0070	Mengembangkan rencana Pemulihan Bencana dan Kontinuitas Operasi untuk sistem yang sedang dikembang kan dan memastika n pengujian sebelum sistem memasuki lingkungan produksi.	dynamodb-autoscali ng-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughpu t yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tuli s yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0070	Mengembangkan rencana Pemulihan Bencana dan Kontinuitas Operasi untuk sistem yang sedang dikembang kan dan memastika n pengujian sebelum sistem memasuki lingkungan produksi.	dynamodb-pitr-enab led	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertah ankan cadangan dengan memastika n bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0070	Mengembangkan rencana Pemulihan Bencana dan Kontinuitas Operasi untuk sistem yang sedang dikembang kan dan memastika n pengujian sebelum sistem memasuki lingkungan produksi.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0070	Mengembangkan rencana Pemulihan Bencana dan Kontinuitas Operasi untuk sistem yang sedang dikembang kan dan memastika n pengujian sebelum sistem memasuki lingkungan produksi.	elb-deletion-prote ction-enabled	Aturan ini memastika n bahwa Elastic Load Balancing memiliki perlindun gan penghapus an yang diaktifka n. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersedi aan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0070	Mengembangkan rencana Pemulihan Bencana dan Kontinuitas Operasi untuk sistem yang sedang dikembang kan dan memastika n pengujian sebelum sistem memasuki lingkungan produksi.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersedi aan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplika si data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastru ktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutk an operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0070	Mengembangkan rencana Pemulihan Bencana dan Kontinuitas Operasi untuk sistem yang sedang dikembang kan dan memastika n pengujian sebelum sistem memasuki lingkungan produksi.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0070	Mengembangkan rencana Pemulihan Bencana dan Kontinuitas Operasi untuk sistem yang sedang dikembang kan dan memastika n pengujian sebelum sistem memasuki lingkungan produksi.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0070	Mengembangkan rencana Pemulihan Bencana dan Kontinuitas Operasi untuk sistem yang sedang dikembang kan dan memastika n pengujian sebelum sistem memasuki lingkungan produksi.	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimpleme ntasikan untuk mencapai persyarat an ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivi tas jika salah satu koneksi Site-to-S ite VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivi tas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0086	Memastikan bahwa penerapan patch keamanan untuk produk komersial yang diintegrasikan ke dalam desain sistem memenuhi jadwal yang ditentukan oleh otoritas manajemen untuk lingkungan operasional yang dimaksud.	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relational Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0086	Memastikan bahwa penerapan patch keamanan untuk produk komersial yang diintegrasikan ke dalam desain sistem memenuhi jadwal yang ditentukan oleh otoritas manajemen untuk lingkungan operasional yang dimaksud.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
T0086	Memastikan bahwa penerapan patch keamanan untuk produk komersial yang diintegrasikan ke dalam desain sistem memenuhi jadwal yang ditentukan oleh otoritas manajemen untuk lingkungan operasional yang dimaksud.	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0086	Memastikan bahwa penerapan patch keamanan untuk produk komersial yang diintegrasikan ke dalam desain sistem memenuhi jadwal yang ditentukan oleh otoritas manajemen untuk lingkungan operasional yang dimaksud.	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0110	Mengidentifikasi dan/atau menentukan apakah insiden keamanan merupakan indikasi pelanggaran hukum yang memerlukan tindakan hukum tertentu.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0110	Mengidentifikasi dan/atau menentukan apakah insiden keamanan merupakan indikasi pelanggaran hukum yang memerlukan tindakan hukum tertentu.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai sebenarnya harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0110	Mengidentifikasi dan/atau menentukan apakah insiden keamanan merupakan indikasi pelanggaran hukum yang memerlukan tindakan hukum tertentu.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0128	Mengintegrasikan kemampuan otomatis untuk memperbar ui atau menambal perangkat lunak sistem di mana praktis dan mengemban gkan proses dan prosedur untuk memperbarui manual dan menambal perangkat lunak sistem berdasarkan persyaratan garis waktu patch saat ini dan yang diproyeks ikan untuk lingkungan operasional sistem.	rds-automatic-mino r-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relationa l Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastika n pembaruan versi minor terbaru ke Relational Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0128	Mengintegrasikan kemampuan otomatis untuk memperbar ui atau menambal perangkat lunak sistem di mana praktis dan mengemban gkan proses dan prosedur untuk memperbarui manual dan menambal perangkat lunak sistem berdasarkan persyaratan garis waktu patch saat ini dan yang diproyeks ikan untuk lingkungan operasional sistem.	ec2- -periksa managedinstance-pa tch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0128	Mengintegrasikan kemampuan otomatis untuk memperbar ui atau menambal perangkat lunak sistem di mana praktis dan mengemban gkan proses dan prosedur untuk memperbarui manual dan menambal perangkat lunak sistem berdasarkan persyaratan garis waktu patch saat ini dan yang diproyeks ikan untuk lingkungan operasional sistem.	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0128	Mengintegrasikan kemampuan otomatis untuk memperbarui atau menambal perangkat lunak sistem di mana praktis dan mengembangkan proses dan prosedur untuk memperbarui manual dan menambal perangkat lunak sistem berdasarkan persyaratan garis waktu patch saat ini dan yang diproyeksikan untuk lingkungan operasional sistem.	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindungi nya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	dibatasi ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositor i data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	s3- account-level-publ ic-access -blok-per iodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain Amazon Elasticsearch Service (Amazon ES) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain Amazon ES dalam VPC Amazon memungkinkan komunikasi yang aman antara Amazon ES dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	secretsmanager-rotation-enabled-check	Aturan ini memastikan AWS rahasia Secrets Manager mengaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0144	Kelola akun, hak jaringan, dan akses ke sistem dan peralatan.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0151	Memantau dan mengevaluasi efektivitas perlindungan keamanan siber perusahaan untuk memastikan bahwa mereka memberikan tingkat perlindungan yang diinginkan.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0151	Memantau dan mengevaluasi efektivitas perlindungan keamanan siber perusahaan untuk memastikan bahwa mereka memberikan tingkat perlindungan yang diinginkan.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai sebenarnya harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0151	Memantau dan mengevaluasi efektivitas perlindungan keamanan siber perusahaan untuk memastikan bahwa mereka memberikan tingkat perlindungan yang diinginkan.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0152	Memantau dan memelihara database untuk memastikan kinerja yang optimal.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0152	Memantau dan memelihara database untuk memastikan kinerja yang optimal.	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0152	Memantau dan memelihara database untuk memastikan kinerja yang optimal.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0152	Memantau dan memelihara database untuk memastikan kinerja yang optimal.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0152	Memantau dan memelihara database untuk memastikan kinerja yang optimal.	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
T0152	Memantau dan memelihara database untuk memastikan kinerja yang optimal.	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relational Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0152	Memantau dan memelihara database untuk memastikan kinerja yang optimal.	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0152	Memantau dan memelihara database untuk memastikan kinerja yang optimal.	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relationa l Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindun gan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersedi aan untuk aplikasi Anda.
T0152	Memantau dan memelihara database untuk memastikan kinerja yang optimal.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0152	Memantau dan memelihara database untuk memastikan kinerja yang optimal.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0152	Memantau dan memelihara database untuk memastikan kinerja yang optimal.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0152	Memantau dan memelihara database untuk memastikan kinerja yang optimal.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0152	Memantau dan memelihara database untuk memastikan kinerja yang optimal.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
T0152	Memantau dan memelihara database untuk memastikan kinerja yang optimal.	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0152	Memantau dan memelihara database untuk memastikan kinerja yang optimal.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0152	Memantau dan memelihara database untuk memastikan kinerja yang optimal.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0152	Memantau dan memelihara database untuk memastikan kinerja yang optimal.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0152	Memantau dan memelihara database untuk memastikan kinerja yang optimal.	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0152	Memantau dan memelihara database untuk memastikan kinerja yang optimal.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
T0152	Memantau dan memelihara database untuk memastikan kinerja yang optimal.	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositor i data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0152	Memantau dan memelihara database untuk memastikan kinerja yang optimal.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
T0152	Memantau dan memelihara database untuk memastikan kinerja yang optimal.	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0153	Memantau kapasitas dan kinerja jaringan.	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0153	Memantau kapasitas dan kinerja jaringan.	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
T0153	Memantau kapasitas dan kinerja jaringan.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0153	Memantau kapasitas dan kinerja jaringan.	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0154	Memantau dan melaporkan penggunaan aset dan sumber daya manajemen pengetahuan.	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.
T0154	Memantau dan melaporkan penggunaan aset dan sumber daya manajemen pengetahuan.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0154	Memantau dan melaporkan penggunaan aset dan sumber daya manajemen pengetahuan.	lambda-concurrency-check	Aturan ini memastikan bahwa batas tinggi dan rendah konkurensi fungsi Lambda ditetapkan. Ini dapat membantu dalam menyusun dasar jumlah permintaan yang dilayani oleh fungsi Anda pada waktu tertentu.
T0154	Memantau dan melaporkan penggunaan aset dan sumber daya manajemen pengetahuan.	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0154	Memantau dan melaporkan penggunaan aset dan sumber daya manajemen pengetahuan.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0154	Memantau dan melaporkan penggunaan aset dan sumber daya manajemen pengetahuan.	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0154	Memantau dan melaporkan penggunaan aset dan sumber daya manajemen pengetahuan.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0154	Memantau dan melaporkan penggunaan aset dan sumber daya manajemen pengetahuan.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0154	Memantau dan melaporkan penggunaan aset dan sumber daya manajemen pengetahuan.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
T0154	Memantau dan melaporkan penggunaan aset dan sumber daya manajemen pengetahuan.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0154	Memantau dan melaporkan penggunaan aset dan sumber daya manajemen pengetahuan.	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0154	Memantau dan melaporkan penggunaan aset dan sumber daya manajemen pengetahuan.	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0154	Memantau dan melaporkan penggunaan aset dan sumber daya manajemen pengetahuan.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
T0154	Memantau dan melaporkan penggunaan aset dan sumber daya manajemen pengetahuan.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0154	Memantau dan melaporkan penggunaan aset dan sumber daya manajemen pengetahuan.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0154	Memantau dan melaporkan penggunaan aset dan sumber daya manajemen pengetahuan.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai sebenarnya harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0154	Memantau dan melaporkan penggunaan aset dan sumber daya manajemen pengetahuan.	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
T0154	Memantau dan melaporkan penggunaan aset dan sumber daya manajemen pengetahuan.	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0154	Memantau dan melaporkan penggunaan aset dan sumber daya manajemen pengetahuan.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0154	Memantau dan melaporkan penggunaan aset dan sumber daya manajemen pengetahuan.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0154	Memantau dan melaporkan penggunaan aset dan sumber daya manajemen pengetahuan.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0154	Memantau dan melaporkan penggunaan aset dan sumber daya manajemen pengetahuan.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0154	Memantau dan melaporkan penggunaan aset dan sumber daya manajemen pengetahuan.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
T0156	Mengawasi dan membuat rekomendasi mengenai manajemen konfigurasi.	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0156	Mengawasi dan membuat rekomendasi mengenai manajemen konfigurasi.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0156	Mengawasi dan membuat rekomendasi mengenai manajemen konfigurasi.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0156	Mengawasi dan membuat rekomendasi mengenai manajemen konfigurasi.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0156	Mengawasi dan membuat rekomendasi mengenai manajemen konfigurasi.	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0156	Mengawasi dan membuat rekomendasi mengenai manajemen konfigurasi.	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0156	Mengawasi dan membuat rekomendasi mengenai manajemen konfigurasi.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0156	Mengawasi dan membuat rekomendasi mengenai manajemen konfigurasi.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0156	Mengawasi dan membuat rekomendasi mengenai manajemen konfigurasi.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0160	Patch kerentana n jaringan untuk memastikan bahwa informasi dilindungi terhadap pihak luar.	rds-automatic-mino r-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relationa l Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastika n pembaruan versi minor terbaru ke Relational Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0160	Patch kerentana n jaringan untuk memastikan bahwa informasi dilindungi terhadap pihak luar.	ec2- -periksa managedinstance-as sociation-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventari s platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0160	Patch kerentana n jaringan untuk memastikan bahwa informasi dilindungi terhadap pihak luar.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0162	Lakukan pencadangan dan pemulihan database untuk memastikan integritas data.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0162	Lakukan pencadangan dan pemulihan database untuk memastikan integritas data.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0162	Lakukan pencadangan dan pemulihan database untuk memastikan integritas data.	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0162	Lakukan pencadang an dan pemulihan database untuk memastikan integritas data.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0162	Lakukan pencadangan dan pemulihan database untuk memastikan integritas data.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0162	Lakukan pencadangan dan pemulihan database untuk memastikan integritas data.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0162	Lakukan pencadangan dan pemulihan database untuk memastikan integritas data.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
T0162	Lakukan pencadangan dan pemulihan database untuk memastikan integritas data.	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0162	Lakukan pencadangan dan pemulihan database untuk memastikan integritas data.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0162	Lakukan pencadangan dan pemulihan database untuk memastikan integritas data.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0162	Lakukan pencadangan dan pemulihan database untuk memastikan integritas data.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0162	Lakukan pencadangan dan pemulihan database untuk memastikan integritas data.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0162	Lakukan pencadangan dan pemulihan database untuk memastikan integritas data.	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0162	Lakukan pencadangan dan pemulihan database untuk memastikan integritas data.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0162	Lakukan pencadang an dan pemulihan database untuk memastikan integritas data.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0166	Lakukan korelasi peristiwa menggunakan informasi yang dikumpulkan dari berbagai sumber dalam perusahaan untuk mendapatkan kesadaran situasional dan menentukan efektivitas serangan yang diamati.	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.
T0166	Lakukan korelasi peristiwa menggunakan informasi yang dikumpulkan dari berbagai sumber dalam perusahaan untuk mendapatkan kesadaran situasional dan menentukan efektivitas serangan yang diamati.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0166	Lakukan korelasi peristiwa menggunakan informasi yang dikumpulkan dari berbagai sumber dalam perusahaan untuk mendapatkan kesadaran situasional dan menentukan efektivitas serangan yang diamati.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0166	Lakukan korelasi peristiwa menggunakan informasi yang dikumpulkan dari berbagai sumber dalam perusahaan untuk mendapatkan kesadaran situasional dan menentukan efektivitas serangan yang diamati.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
T0166	Lakukan korelasi peristiwa menggunakan informasi yang dikumpulkan dari berbagai sumber dalam perusahaan untuk mendapatkan kesadaran situasional dan menentukan efektivitas serangan yang diamati.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0166	Lakukan korelasi peristiwa menggunakan informasi yang dikumpulkan dari berbagai sumber dalam perusahaan untuk mendapatkan kesadaran situasional dan menentukan efektivitas serangan yang diamati.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
T0166	Lakukan korelasi peristiwa menggunakan informasi yang dikumpulkan dari berbagai sumber dalam perusahaan untuk mendapatkan kesadaran situasional dan menentukan efektivitas serangan yang diamati.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0166	Lakukan korelasi peristiwa menggunakan informasi yang dikumpulkan dari berbagai sumber dalam perusahaan untuk mendapatkan kesadaran situasional dan menentukan efektivitas serangan yang diamati.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
T0166	Lakukan korelasi peristiwa menggunakan informasi yang dikumpulkan dari berbagai sumber dalam perusahaan untuk mendapatkan kesadaran situasional dan menentukan efektivitas serangan yang diamati.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0166	Lakukan korelasi peristiwa menggunakan informasi yang dikumpulkan dari berbagai sumber dalam perusahaan untuk mendapatkan kesadaran situasional dan menentukan efektivitas serangan yang diamati.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0166	Lakukan korelasi peristiwa menggunakan informasi yang dikumpulkan dari berbagai sumber dalam perusahaan untuk mendapatkan kesadaran situasional dan menentukan efektivitas serangan yang diamati.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0166	Lakukan korelasi peristiwa menggunakan informasi yang dikumpulkan dari berbagai sumber dalam perusahaan untuk mendapatkan kesadaran situasional dan menentukan efektivitas serangan yang diamati.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0166	Lakukan korelasi peristiwa menggunakan informasi yang dikumpulkan dari berbagai sumber dalam perusahaan untuk mendapatkan kesadaran situasional dan menentukan efektivitas serangan yang diamati.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0168	Lakukan perbandingan hash terhadap database yang sudah mapan.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0195	Menyediakan aliran informasi yang relevan yang dikelola (melalui portal berbasis web atau cara lain) berdasarkan persyaratan misi.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0195	Menyediakan aliran informasi yang relevan yang dikelola (melalui portal berbasis web atau cara lain) berdasarkan persyaratan misi.	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindungi nya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0195	Menyediakan aliran informasi yang relevan yang dikelola (melalui portal berbasis web atau cara lain) berdasarkan persyaratan misi.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfig urasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0195	Menyediakan aliran informasi yang relevan yang dikelola (melalui portal berbasis web atau cara lain) berdasarkan persyaratan misi.	dibatasi ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0195	Menyediakan aliran informasi yang relevan yang dikelola (melalui portal berbasis web atau cara lain) berdasarkan persyaratan misi.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0195	Menyediakan aliran informasi yang relevan yang dikelola (melalui portal berbasis web atau cara lain) berdasarkan persyaratan misi.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
T0195	Menyediakan aliran informasi yang relevan yang dikelola (melalui portal berbasis web atau cara lain) berdasarkan persyaratan misi.	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositor i data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0195	Menyediakan aliran informasi yang relevan yang dikelola (melalui portal berbasis web atau cara lain) berdasarkan persyaratan misi.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0195	Menyediakan aliran informasi yang relevan yang dikelola (melalui portal berbasis web atau cara lain) berdasarkan persyaratan misi.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
T0195	Menyediakan aliran informasi yang relevan yang dikelola (melalui portal berbasis web atau cara lain) berdasarkan persyaratan misi.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0195	Menyediakan aliran informasi yang relevan yang dikelola (melalui portal berbasis web atau cara lain) berdasarkan persyaratan misi.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
T0195	Menyediakan aliran informasi yang relevan yang dikelola (melalui portal berbasis web atau cara lain) berdasarkan persyaratan misi.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0195	Menyediakan aliran informasi yang relevan yang dikelola (melalui portal berbasis web atau cara lain) berdasarkan persyaratan misi.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
T0195	Menyediakan aliran informasi yang relevan yang dikelola (melalui portal berbasis web atau cara lain) berdasarkan persyaratan misi.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0195	Menyediakan aliran informasi yang relevan yang dikelola (melalui portal berbasis web atau cara lain) berdasarkan persyaratan misi.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0195	Menyediakan aliran informasi yang relevan yang dikelola (melalui portal berbasis web atau cara lain) berdasarkan persyaratan misi.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0195	Menyediakan aliran informasi yang relevan yang dikelola (melalui portal berbasis web atau cara lain) berdasarkan persyaratan misi.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain Amazon Elasticsearch Service (Amazon ES) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain Amazon ES dalam VPC Amazon memungkinkan komunikasi yang aman antara Amazon ES dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0195	Menyediakan aliran informasi yang relevan yang dikelola (melalui portal berbasis web atau cara lain) berdasarkan persyaratan misi.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
T0195	Menyediakan aliran informasi yang relevan yang dikelola (melalui portal berbasis web atau cara lain) berdasarkan persyaratan misi.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0195	Menyediakan aliran informasi yang relevan yang dikelola (melalui portal berbasis web atau cara lain) berdasarkan persyaratan misi.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0195	Menyediakan aliran informasi yang relevan yang dikelola (melalui portal berbasis web atau cara lain) berdasarkan persyaratan misi.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0195	Menyediakan aliran informasi yang relevan yang dikelola (melalui portal berbasis web atau cara lain) berdasarkan persyaratan misi.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
T0195	Menyediakan aliran informasi yang relevan yang dikelola (melalui portal berbasis web atau cara lain) berdasarkan persyaratan misi.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0195	Menyediakan aliran informasi yang relevan yang dikelola (melalui portal berbasis web atau cara lain) berdasarkan persyaratan misi.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
T0195	Menyediakan aliran informasi yang relevan yang dikelola (melalui portal berbasis web atau cara lain) berdasarkan persyaratan misi.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0195	Menyediakan aliran informasi yang relevan yang dikelola (melalui portal berbasis web atau cara lain) berdasarkan persyaratan misi.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0195	Menyediakan aliran informasi yang relevan yang dikelola (melalui portal berbasis web atau cara lain) berdasarkan persyaratan misi.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0215	Kenali kemungkin an pelanggaran keamanan dan ambil tindakan yang tepat untuk melaporkan insiden tersebut, sebagaima na diperlukan.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0244	Verifikasi bahwa postur software/network/system keamanan aplikasi diterapkan sebagaimana dinyatakan, dokumen penyimpangan, dan merekomendasikan tindakan yang diperlukan untuk memperbaiki penyimpangan tersebut.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0244	Verifikasi bahwa postur software/ network/system keamanan aplikasi diterapkan sebagaima na dinyatakan, dokumen penyimpan gan, dan merekomen dasikan tindakan yang diperlukan untuk memperbai ki penyimpangan tersebut.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0244	Verifikasi bahwa postur software/ network/system keamanan aplikasi diterapkan sebagaima na dinyatakan, dokumen penyimpan gan, dan merekomen dasikan tindakan yang diperlukan untuk memperbai ki penyimpangan tersebut.	ec2- -periksa managedinstance-as sociation-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventari s platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0258	Memberikan deteksi, identifikasi, dan peringatan tepat waktu kemungkin an serangan/ intrusi, aktivitas anomali, dan aktivitas penyalahgunaan dan membedakan insiden dan peristiwa ini dari aktivitas jinak.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0259	Gunakan alat pertahanan cyber untuk pemantauan terus-menerus dan analisis aktivitas sistem untuk mengidentifikasi aktivitas berbahaya.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0262	Gunakan defense-in-depth prinsip dan praktik yang disetujui (misalnya, defense-in-multiple tempat, pertahanan berlapis, ketahanan keamanan).	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0262	Gunakan defense-in-depth prinsip dan praktik yang disetujui (misalnya, defense-in-multiple tempat, pertahanan berlapis, ketahanan keamanan).	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindungi nya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0262	Gunakan defense-in-depth prinsip dan praktik yang disetujui (misalnya, defense-in-multiple tempat, pertahanan berlapis, ketahanan keamanan).	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0262	Gunakan defense-in-depth prinsip dan praktik yang disetujui (misalnya, defense-in-multiple tempat, pertahanan berlapis, ketahanan keamanan).	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0262	Gunakan defense-in-depth prinsip dan praktik yang disetujui (misalnya, defense-in-multiple tempat, pertahanan berlapis, ketahanan keamanan).	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
T0262	Gunakan defense-in-depth prinsip dan praktik yang disetujui (misalnya, defense-in-multiple tempat, pertahanan berlapis, ketahanan keamanan).	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositori data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0262	Gunakan defense-in-depth prinsip dan praktik yang disetujui (misalnya, defense-in-multiple tempat, pertahanan berlapis, ketahanan keamanan).	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0262	Gunakan defense-in-depth prinsip dan praktik yang disetujui (misalnya, defense-in-multiple tempat, pertahanan berlapis, ketahanan keamanan).	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
T0262	Gunakan defense-in-depth prinsip dan praktik yang disetujui (misalnya, defense-in-multiple tempat, pertahanan berlapis, ketahanan keamanan).	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0262	Gunakan defense-in-depth prinsip dan praktik yang disetujui (misalnya, defense-in-multiple tempat, pertahanan berlapis, ketahanan keamanan).	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
T0262	Gunakan defense-in-depth prinsip dan praktik yang disetujui (misalnya, defense-in-multiple tempat, pertahanan berlapis, ketahanan keamanan).	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0262	Gunakan defense-in-depth prinsip dan praktik yang disetujui (misalnya, defense-in-multiple tempat, pertahanan berlapis, ketahanan keamanan).	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
T0262	Gunakan defense-in-depth prinsip dan praktik yang disetujui (misalnya, defense-in-multiple tempat, pertahanan berlapis, ketahanan keamanan).	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0262	Gunakan defense-in-depth prinsip dan praktik yang disetujui (misalnya, defense-in-multiple tempat, pertahanan berlapis, ketahanan keamanan).	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0262	Gunakan defense-in-depth prinsip dan praktik yang disetujui (misalnya, defense-in-multiple tempat, pertahanan berlapis, ketahanan keamanan).	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigurasi ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0262	Gunakan defense-in-depth prinsip dan praktik yang disetujui (misalnya, defense-in-multiple tempat, pertahanan berlapis, ketahanan keamanan).	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain Amazon Elasticsearch Service (Amazon ES) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain Amazon ES dalam VPC Amazon memungkinkan komunikasi yang aman antara Amazon ES dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0262	Gunakan defense-in-depth prinsip dan praktik yang disetujui (misalnya, defense-in-multiple tempat, pertahanan berlapis, ketahanan keamanan).	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
T0262	Gunakan defense-in-depth prinsip dan praktik yang disetujui (misalnya, defense-in-multiple tempat, pertahanan berlapis, ketahanan keamanan).	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0262	Gunakan defense-in-depth prinsip dan praktik yang disetujui (misalnya, defense-in-multiple tempat, pertahanan berlapis, ketahanan keamanan).	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0262	Gunakan defense-in-depth prinsip dan praktik yang disetujui (misalnya, defense-in-multiple tempat, pertahanan berlapis, ketahanan keamanan).	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0262	Gunakan defense-in-depth prinsip dan praktik yang disetujui (misalnya, defense-in-multiple tempat, pertahanan berlapis, ketahanan keamanan).	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
T0262	Gunakan defense-in-depth prinsip dan praktik yang disetujui (misalnya, defense-in-multiple tempat, pertahanan berlapis, ketahanan keamanan).	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0262	Gunakan defense-in-depth prinsip dan praktik yang disetujui (misalnya, defense-in-multiple tempat, pertahanan berlapis, ketahanan keamanan).	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
T0262	Gunakan defense-in-depth prinsip dan praktik yang disetujui (misalnya, defense-in-multiple tempat, pertahanan berlapis, ketahanan keamanan).	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0262	Gunakan defense-in-depth prinsip dan praktik yang disetujui (misalnya, defense-in-multiple tempat, pertahanan berlapis, ketahanan keamanan).	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0262	Gunakan defense-in-depth prinsip dan praktik yang disetujui (misalnya, defense-in-multiple tempat, pertahanan berlapis, ketahanan keamanan).	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindungi nya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relational Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositor i data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild . Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredenal masuk dalam lingkungan proyek Codebuild . AWS Gunakan OAuth alih-alih token akses pribadi atau kredensyal masuk untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain Amazon Elasticsearch Service (Amazon ES) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain Amazon ES dalam VPC Amazon memungkinkan komunikasi yang aman antara Amazon ES dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0284	Merancang dan mengembangkan alat/teknologi baru yang terkait dengan keamanan siber.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0306	Mendukung manajemen insiden, manajemen tingkat layanan, manajemen perubahan, manajemen rilis, manajemen kontinuitas, dan manajemen ketersediaan untuk database dan sistem manajemen data.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0306	Mendukung manajemen insiden, manajemen tingkat layanan, manajemen perubahan, manajemen rilis, manajemen kontinuitas, dan manajemen ketersediaan untuk database dan sistem manajemen data.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai sebenarnya harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0306	Mendukung manajemen insiden, manajemen tingkat layanan, manajemen perubahan, manajemen rilis, manajemen kontinuitas, dan manajemen ketersediaan untuk database dan sistem manajemen data.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0314	Mengembangkan konteks keamanan sistem, Konsep Operasi keamanan sistem awal (CONOPS), dan tentukan persyaratan keamanan sistem dasar sesuai dengan persyaratan keamanan siber yang berlaku.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0314	Mengembangkan konteks keamanan sistem, Konsep Operasi keamanan sistem awal (CONOPS), dan tentukan persyaratan keamanan sistem dasar sesuai dengan persyaratan keamanan siber yang berlaku.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0314	Mengembangkan konteks keamanan sistem, Konsep Operasi keamanan sistem awal (CONOPS), dan tentukan persyaratan keamanan sistem dasar sesuai dengan persyaratan keamanan siber yang berlaku.	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.
T0314	Mengembangkan konteks keamanan sistem, Konsep Operasi keamanan sistem awal (CONOPS), dan tentukan persyaratan keamanan sistem dasar sesuai dengan persyaratan keamanan siber yang berlaku.	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0314	Mengembangkan konteks keamanan sistem, Konsep Operasi keamanan sistem awal (CONOPS), dan tentukan persyaratan keamanan sistem dasar sesuai dengan persyaratan keamanan siber yang berlaku.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0314	Mengembangkan konteks keamanan sistem, Konsep Operasi keamanan sistem awal (CONOPS), dan tentukan persyaratan keamanan sistem dasar sesuai dengan persyaratan keamanan siber yang berlaku.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0333	Lakukan analisis dan pelaporan tren pertahanan dunia maya.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0333	Lakukan analisis dan pelaporan tren pertahanan dunia maya.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0347	Menilai validitas data sumber dan temuan selanjutnya.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0358	Merancang dan mengembangkan administrasi sistem dan fungsionalitas manajemen untuk pengguna akses istimewa.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0358	Merancang dan mengembangkan administrasi sistem dan fungsionalitas manajemen untuk pengguna akses istimewa.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0358	Merancang dan mengembangkan administrasi sistem dan fungsionalitas manajemen untuk pengguna akses istimewa.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
T0358	Merancang dan mengembangkan administrasi sistem dan fungsionalitas manajemen untuk pengguna akses istimewa.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0358	Merancang dan mengembangkan administrasi sistem dan fungsionalitas manajemen untuk pengguna akses istimewa.	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
T0358	Merancang dan mengembangkan administrasi sistem dan fungsionalitas manajemen untuk pengguna akses istimewa.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0358	Merancang dan mengembangkan administrasi sistem dan fungsionalitas manajemen untuk pengguna akses istimewa.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0358	Merancang dan mengembangkan administrasi sistem dan fungsionalitas manajemen untuk pengguna akses istimewa.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.
T0376	Menetapkan, sumber daya, mengimplementasikan, dan menilai program manajemen tenaga kerja cyber sesuai dengan persyaratan organisasi.	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0376	Menetapkan, sumber daya, mengimple mentasikan, dan menilai program manajemen tenaga kerja cyber sesuai dengan persyaratan organisasi.	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.
T0376	Menetapkan, sumber daya, mengimple mentasikan, dan menilai program manajemen tenaga kerja cyber sesuai dengan persyaratan organisasi.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0376	Menetapkan, sumber daya, mengimple mentasikan, dan menilai program manajemen tenaga kerja cyber sesuai dengan persyaratan organisasi.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0376	Menetapkan, sumber daya, mengimple mentasikan, dan menilai program manajemen tenaga kerja cyber sesuai dengan persyaratan organisasi.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0376	Menetapkan, sumber daya, mengimple mentasikan, dan menilai program manajemen tenaga kerja cyber sesuai dengan persyaratan organisasi.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0376	Menetapkan, sumber daya, mengimple mentasikan, dan menilai program manajemen tenaga kerja cyber sesuai dengan persyaratan organisasi.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
T0376	Menetapkan, sumber daya, mengimple mentasikan, dan menilai program manajemen tenaga kerja cyber sesuai dengan persyaratan organisasi.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0376	Menetapkan, sumber daya, mengimple mentasikan, dan menilai program manajemen tenaga kerja cyber sesuai dengan persyaratan organisasi.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
T0376	Menetapkan, sumber daya, mengimple mentasikan, dan menilai program manajemen tenaga kerja cyber sesuai dengan persyaratan organisasi.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteks i aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0376	Menetapkan, sumber daya, mengimple mentasikan, dan menilai program manajemen tenaga kerja cyber sesuai dengan persyaratan organisasi.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0376	Menetapkan, sumber daya, mengimple mentasikan, dan menilai program manajemen tenaga kerja cyber sesuai dengan persyaratan organisasi.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
T0376	Menetapkan, sumber daya, mengimple mentasikan, dan menilai program manajemen tenaga kerja cyber sesuai dengan persyaratan organisasi.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0376	Menetapkan, sumber daya, mengimple mentasikan, dan menilai program manajemen tenaga kerja cyber sesuai dengan persyaratan organisasi.	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
T0376	Menetapkan, sumber daya, mengimplementasikan, dan menilai program manajemen tenaga kerja cyber sesuai dengan persyaratan organisasi.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0376	Menetapkan, sumber daya, mengimple mentasikan, dan menilai program manajemen tenaga kerja cyber sesuai dengan persyaratan organisasi.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0376	Menetapkan, sumber daya, mengimple mentasikan, dan menilai program manajemen tenaga kerja cyber sesuai dengan persyaratan organisasi.	iam-user-no-policies-periksa	Aturan ini memastika n kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapka n hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0376	Menetapkan, sumber daya, mengimple mentasikan, dan menilai program manajemen tenaga kerja cyber sesuai dengan persyaratan organisasi.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediak an metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinc i untuk permintaa n yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0376	Menetapkan, sumber daya, mengimple mentasikan, dan menilai program manajemen tenaga kerja cyber sesuai dengan persyaratan organisasi.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
T0416	Aktifkan aplikasi dengan kunci publik dengan memanfaat kan pustaka infrastru ktur kunci publik (PKI) yang ada dan menggabungkan fungsi manajemen sertifikat dan enkripsi bila diperlukan.	acm-certificate-ex piration-check	Pastikan integritas jaringan dilindungi dengan memastika n sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExp iration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0416	Aktifkan aplikasi dengan kunci publik dengan memanfaat kan pustaka infrastru ktur kunci publik (PKI) yang ada dan menggabungkan fungsi manajemen sertifikat dan enkripsi bila diperlukan.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
T0416	Aktifkan aplikasi dengan kunci publik dengan memanfaat kan pustaka infrastru ktur kunci publik (PKI) yang ada dan menggabungkan fungsi manajemen sertifikat dan enkripsi bila diperlukan.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-n ode enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkrip si memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0416	Aktifkan aplikasi dengan kunci publik dengan memanfaat kan pustaka infrastru ktur kunci publik (PKI) yang ada dan menggabungkan fungsi manajemen sertifikat dan enkripsi bila diperlukan.	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0416	Aktifkan aplikasi dengan kunci publik dengan memanfaat kan pustaka infrastru ktur kunci publik (PKI) yang ada dan menggabungkan fungsi manajemen sertifikat dan enkripsi bila diperlukan.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
T0416	Aktifkan aplikasi dengan kunci publik dengan memanfaat kan pustaka infrastru ktur kunci publik (PKI) yang ada dan menggabungkan fungsi manajemen sertifikat dan enkripsi bila diperlukan.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0416	Aktifkan aplikasi dengan kunci publik dengan memanfaat kan pustaka infrastru ktur kunci publik (PKI) yang ada dan menggabungkan fungsi manajemen sertifikat dan enkripsi bila diperlukan.	opensearch-node-to -node-pemeriksaan enkripsi-	Pastikan node-to-n ode enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkrip si memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
T0416	Aktifkan aplikasi dengan kunci publik dengan memanfaat kan pustaka infrastru ktur kunci publik (PKI) yang ada dan menggabungkan fungsi manajemen sertifikat dan enkripsi bila diperlukan.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0416	Aktifkan aplikasi dengan kunci publik dengan memanfaat kan pustaka infrastru ktur kunci publik (PKI) yang ada dan menggabungkan fungsi manajemen sertifikat dan enkripsi bila diperlukan.	s3- bucket-ssl-request s-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
T0416	Aktifkan aplikasi dengan kunci publik dengan memanfaat kan pustaka infrastru ktur kunci publik (PKI) yang ada dan menggabungkan fungsi manajemen sertifikat dan enkripsi bila diperlukan.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0421	Mengelola pengindeks/katalog, penyimpanan, dan akses pengetahuan organisasi eksplisit (misalnya, dokumen hard copy, file digital).	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
T0421	Mengelola pengindeks/katalog, penyimpanan, dan akses pengetahuan organisasi eksplisit (misalnya, dokumen hard copy, file digital).	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0421	Mengelola pengindeks/katalog, penyimpanan, dan akses pengetahuan organisasi eksplisit (misalnya, dokumen hard copy, file digital).	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
T0421	Mengelola pengindeks/katalog, penyimpanan, dan akses pengetahuan organisasi eksplisit (misalnya, dokumen hard copy, file digital).	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0421	Mengelola pengindeks/katalog, penyimpanan, dan akses pengetahuan organisasi eksplisit (misalnya, dokumen hard copy, file digital).	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
T0421	Mengelola pengindeks/katalog, penyimpanan, dan akses pengetahuan organisasi eksplisit (misalnya, dokumen hard copy, file digital).	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0421	Mengelola pengindeks/katalog, penyimpanan, dan akses pengetahuan organisasi eksplisit (misalnya, dokumen hard copy, file digital).	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
T0421	Mengelola pengindeks/katalog, penyimpanan, dan akses pengetahuan organisasi eksplisit (misalnya, dokumen hard copy, file digital).	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0421	Mengelola pengindeks/katalog, penyimpanan, dan akses pengetahuan organisasi eksplisit (misalnya, dokumen hard copy, file digital).	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0421	Mengelola pengindeks/katalog, penyimpanan, dan akses pengetahuan organisasi eksplisit (misalnya, dokumen hard copy, file digital).	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0421	Mengelola pengindeks/katalog, penyimpanan, dan akses pengetahuan organisasi eksplisit (misalnya, dokumen hard copy, file digital).	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
T0421	Mengelola pengindeks/katalog, penyimpanan, dan akses pengetahuan organisasi eksplisit (misalnya, dokumen hard copy, file digital).	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0421	Mengelola pengindeks/katalog, penyimpanan, dan akses pengetahuan organisasi eksplisit (misalnya, dokumen hard copy, file digital).	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0421	Mengelola pengindeks/katalog, penyimpanan, dan akses pengetahuan organisasi eksplisit (misalnya, dokumen hard copy, file digital).	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktifkan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediakan sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0421	Mengelola pengindeks/katalog, penyimpanan, dan akses pengetahuan organisasi eksplisit (misalnya, dokumen hard copy, file digital).	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know.	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know.	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain Amazon Elasticsearch Service (Amazon ES) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain Amazon ES dalam VPC Amazon memungkinkan komunikasi yang aman antara Amazon ES dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0475	Menilai kontrol akses yang memadai berdasarkan prinsip-prinsip hak istimewa yang paling rendah dan need-to-know	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
T0489	Menerapkan langkah-langkah keamanan sistem sesuai dengan prosedur yang ditetapkan untuk memastikan kerahasiaan, integritas, ketersediaan, otentikasi, dan non-penolakan.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0489	Menerapkan langkah-langkah keamanan sistem sesuai dengan prosedur yang ditetapkan untuk memastikan kerahasiaan, integrita s, ketersediaan, otentikasi, dan non-penolakan.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0489	Menerapkan langkah-langkah keamanan sistem sesuai dengan prosedur yang ditetapkan untuk memastikan kerahasiaan, integritas, ketersediaan, otentikasi, dan non-penolakan.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
T0489	Menerapkan langkah-langkah keamanan sistem sesuai dengan prosedur yang ditetapkan untuk memastikan kerahasiaan, integritas, ketersediaan, otentikasi, dan non-penolakan.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0489	Menerapkan langkah-langkah keamanan sistem sesuai dengan prosedur yang ditetapkan untuk memastikan kerahasiaan, integrita s, ketersediaan, otentikasi, dan non-penolakan.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
T0489	Menerapkan langkah-langkah keamanan sistem sesuai dengan prosedur yang ditetapkan untuk memastikan kerahasiaan, integrita s, ketersediaan, otentikasi, dan non-penolakan.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0489	Menerapkan langkah-langkah keamanan sistem sesuai dengan prosedur yang ditetapkan untuk memastikan kerahasiaan, integritas, ketersediaan, otentikasi, dan non-penolakan.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
T0489	Menerapkan langkah-langkah keamanan sistem sesuai dengan prosedur yang ditetapkan untuk memastikan kerahasiaan, integritas, ketersediaan, otentikasi, dan non-penolakan.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0489	Menerapkan langkah-langkah keamanan sistem sesuai dengan prosedur yang ditetapkan untuk memastikan kerahasiaan, integrita s, ketersediaan, otentikasi, dan non-penolakan.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0489	Menerapkan langkah-langkah keamanan sistem sesuai dengan prosedur yang ditetapkan untuk memastikan kerahasiaan, integritas, ketersediaan, otentikasi, dan non-penolakan.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0489	Menerapkan langkah-langkah keamanan sistem sesuai dengan prosedur yang ditetapkan untuk memastikan kerahasiaan, integritas, ketersediaan, otentikasi, dan non-penolakan.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0489	Menerapkan langkah-langkah keamanan sistem sesuai dengan prosedur yang ditetapkan untuk memastikan kerahasiaan, integrita s, ketersediaan, otentikasi, dan non-penolakan.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0491	Instal dan konfigura si perangkat keras, perangkat lunak, dan peralatan periferal untuk pengguna sistem sesuai dengan standar organisasi.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0491	Instal dan konfigura si perangkat keras, perangkat lunak, dan peralatan periferal untuk pengguna sistem sesuai dengan standar organisasi.	ec2- -periksa managedinstance-as sociation-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventari s platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0491	Instal dan konfigura si perangkat keras, perangkat lunak, dan peralatan periferal untuk pengguna sistem sesuai dengan standar organisasi.	ec2- -periksa managedinstance-pa tch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0503	Pantau sumber data eksternal (misalnya, situs vendor pertahana n dunia maya, Tim Tanggap Darurat Komputer, Fokus Keamanan) untuk mempertahankan mata uang kondisi ancaman pertahana n dunia maya dan menentukan masalah keamanan mana yang mungkin berdampak pada perusahaan.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
T0509	Lakukan penilaian risiko keamanan informasi.	annual-risk-assess ment-performed (pemeriksaan proses)	Lakukan penilaian risiko tahunan pada organisasi Anda. Penilaian risiko dapat membantu dalam menentuka n kemungkinan dan dampak dari risiko dan/atau kerentana n yang diidentifikasi yang mempengaruhi suatu organisasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-n ode enkripsi untuk Amazon Elasticsearch Service diaktifkan. Node-to-nodeenkrip si memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	iam-user-no-policies-periksa	Aturan ini memastika n kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapka n hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk domain Amazon Elasticsearch Service (Amazon ES) Anda.
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk Amazon Elasticsearch Service diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	elasticsearch-encr ypted-at-rest	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk domain Amazon Elasticsearch Service (Amazon ES) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0553	Menerapkan fungsi keamanan siber (misalnya, enkripsi, kontrol akses, dan manajemen identitas) untuk mengurangi peluang eksploitasi.	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
T0557	Integrasikan fungsi manajemen kunci yang terkait dengan dunia maya.	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0557	Integrasikan fungsi manajemen kunci yang terkait dengan dunia maya.	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0576	Menilai semua sumber intelijen dan merekomen dasikan target untuk mendukung tujuan operasi cyber.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0609	Melakukan akses yang memungkinkan komputer nirkabel dan jaringan digital.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0609	Melakukan akses yang memungkinkan komputer nirkabel dan jaringan digital.	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindungi nya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0609	Melakukan akses yang memungkinkan komputer nirkabel dan jaringan digital.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
T0609	Melakukan akses yang memungkinkan komputer nirkabel dan jaringan digital.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0609	Melakukan akses yang memungkinkan komputer nirkabel dan jaringan digital.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
T0609	Melakukan akses yang memungkinkan komputer nirkabel dan jaringan digital.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0609	Melakukan akses yang memungkinkan komputer nirkabel dan jaringan digital.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain Amazon Elasticsearch Service (Amazon ES) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain Amazon ES dalam VPC Amazon memungkinkan komunikasi yang aman antara Amazon ES dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
T0609	Melakukan akses yang memungkinkan komputer nirkabel dan jaringan digital.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0609	Melakukan akses yang memungkinkan komputer nirkabel dan jaringan digital.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0609	Melakukan akses yang memungkinkan komputer nirkabel dan jaringan digital.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0609	Melakukan akses yang memungkinkan komputer nirkabel dan jaringan digital.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0609	Melakukan akses yang memungkinkan komputer nirkabel dan jaringan digital.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0609	Melakukan akses yang memungkinkan komputer nirkabel dan jaringan digital.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
T0609	Melakukan akses yang memungkinkan komputer nirkabel dan jaringan digital.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0609	Melakukan akses yang memungkinkan komputer nirkabel dan jaringan digital.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
T0609	Melakukan akses yang memungkinkan komputer nirkabel dan jaringan digital.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0609	Melakukan akses yang memungkinkan komputer nirkabel dan jaringan digital.	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositor i data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0609	Melakukan akses yang memungkinkan komputer nirkabel dan jaringan digital.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0609	Melakukan akses yang memungkinkan komputer nirkabel dan jaringan digital.	s3- account-level-publ ic-access -blok-per iodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0609	Melakukan akses yang memungkinkan komputer nirkabel dan jaringan digital.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
T0609	Melakukan akses yang memungkinkan komputer nirkabel dan jaringan digital.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0609	Melakukan akses yang memungkinkan komputer nirkabel dan jaringan digital.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0609	Melakukan akses yang memungkinkan komputer nirkabel dan jaringan digital.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0609	Melakukan akses yang memungkinkan komputer nirkabel dan jaringan digital.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0609	Melakukan akses yang memungkinkan komputer nirkabel dan jaringan digital.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain Amazon Elasticsearch Service (Amazon ES) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain Amazon ES dalam VPC Amazon memungkinkan komunikasi yang aman antara Amazon ES dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0609	Melakukan akses yang memungkinkan komputer nirkabel dan jaringan digital.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0616	Melakukan pengintai an jaringan dan analisis kerentana n sistem dalam jaringan.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0686	Identifikasi kerentanan ancaman.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0686	Identifikasi kerentana n ancaman.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
T0706	Kumpulkan informasi tentang jaringan melalui teknik tradisional dan alternatif, (misalnya, analisis jejaring sosial, rantai panggilan, analisis lalu lintas.)	cw-loggroup-retent ion-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonst ruksi dan mengident ifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0706	Kumpulkan informasi tentang jaringan melalui teknik tradisional dan alternatif, (misalnya, analisis jejaring sosial, rantai panggilan, analisis lalu lintas.)	elasticsearch-logs-to-cloudwatch	Pastikan domain layanan Amazon Elasticsearch mengaktifkan log kesalahan dan dialirkan ke Log CloudWatch Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
T0706	Kumpulkan informasi tentang jaringan melalui teknik tradisional dan alternatif, (misalnya, analisis jejaring sosial, rantai panggilan, analisis lalu lintas.)	lambda-concurrency-check	Aturan ini memastikan bahwa batas tinggi dan rendah konkurensi fungsi Lambda ditetapkan. Ini dapat membantu dalam menyusun dasar jumlah permintaan yang dilayani oleh fungsi Anda pada waktu tertentu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0706	Kumpulkan informasi tentang jaringan melalui teknik tradisional dan alternatif, (misalnya, analisis jejaring sosial, rantai panggilan, analisis lalu lintas.)	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0706	Kumpulkan informasi tentang jaringan melalui teknik tradisional dan alternatif, (misalnya, analisis jejaring sosial, rantai panggilan, analisis lalu lintas.)	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0706	Kumpulkan informasi tentang jaringan melalui teknik tradisional dan alternatif, (misalnya, analisis jejaring sosial, rantai panggilan, analisis lalu lintas.)	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0706	Kumpulkan informasi tentang jaringan melalui teknik tradisional dan alternatif, (misalnya, analisis jejaring sosial, rantai panggilan, analisis lalu lintas.)	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0706	Kumpulkan informasi tentang jaringan melalui teknik tradisional dan alternatif, (misalnya, analisis jejaring sosial, rantai panggilan, analisis lalu lintas.)	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0706	Kumpulkan informasi tentang jaringan melalui teknik tradisional dan alternatif, (misalnya, analisis jejaring sosial, rantai panggilan, analisis lalu lintas.)	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
T0706	Kumpulkan informasi tentang jaringan melalui teknik tradisional dan alternatif, (misalnya, analisis jejaring sosial, rantai panggilan, analisis lalu lintas.)	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0706	Kumpulkan informasi tentang jaringan melalui teknik tradisional dan alternatif, (misalnya, analisis jejaring sosial, rantai panggilan, analisis lalu lintas.)	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0706	Kumpulkan informasi tentang jaringan melalui teknik tradisional dan alternatif, (misalnya, analisis jejaring sosial, rantai panggilan, analisis lalu lintas.)	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0706	Kumpulkan informasi tentang jaringan melalui teknik tradisional dan alternatif, (misalnya, analisis jejaring sosial, rantai panggilan, analisis lalu lintas.)	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
T0706	Kumpulkan informasi tentang jaringan melalui teknik tradisional dan alternatif, (misalnya, analisis jejaring sosial, rantai panggilan, analisis lalu lintas.)	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0706	Kumpulkan informasi tentang jaringan melalui teknik tradisional dan alternatif, (misalnya, analisis jejaring sosial, rantai panggilan, analisis lalu lintas.)	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0706	Kumpulkan informasi tentang jaringan melalui teknik tradisional dan alternatif, (misalnya, analisis jejaring sosial, rantai panggilan, analisis lalu lintas.)	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai sebenarnya harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0706	Kumpulkan informasi tentang jaringan melalui teknik tradisional dan alternatif, (misalnya, analisis jejaring sosial, rantai panggilan, analisis lalu lintas.)	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
T0706	Kumpulkan informasi tentang jaringan melalui teknik tradisional dan alternatif, (misalnya, analisis jejaring sosial, rantai panggilan, analisis lalu lintas.)	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0706	Kumpulkan informasi tentang jaringan melalui teknik tradisional dan alternatif, (misalnya, analisis jejaring sosial, rantai panggilan, analisis lalu lintas.)	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0706	Kumpulkan informasi tentang jaringan melalui teknik tradisional dan alternatif, (misalnya, analisis jejaring sosial, rantai panggilan, analisis lalu lintas.)	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0706	Kumpulkan informasi tentang jaringan melalui teknik tradisional dan alternatif, (misalnya, analisis jejaring sosial, rantai panggilan, analisis lalu lintas.)	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0706	Kumpulkan informasi tentang jaringan melalui teknik tradisional dan alternatif, (misalnya, analisis jejaring sosial, rantai panggilan, analisis lalu lintas.)	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0706	Kumpulkan informasi tentang jaringan melalui teknik tradisional dan alternatif, (misalnya, analisis jejaring sosial, rantai panggilan, analisis lalu lintas.)	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0777	Profil jaringan atau administrator sistem dan aktivitas mereka.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0805	Laporkan peristiwa dan intrusi jaringan signifikan yang diturunkan dari intelijen.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
T0877	Bekerja secara kooperatif dengan unit organisasi yang berlaku dalam mengawasi hak akses informasi konsumen	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0877	Bekerja secara kooperatif dengan unit organisasi yang berlaku dalam mengawasi hak akses informasi konsumen	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0877	Bekerja secara kooperatif dengan unit organisasi yang berlaku dalam mengawasi hak akses informasi konsumen	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0877	Bekerja secara kooperatif dengan unit organisasi yang berlaku dalam mengawasi hak akses informasi konsumen	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
T0877	Bekerja secara kooperatif dengan unit organisasi yang berlaku dalam mengawasi hak akses informasi konsumen	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0877	Bekerja secara kooperatif dengan unit organisasi yang berlaku dalam mengawasi hak akses informasi konsumen	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0877	Bekerja secara kooperatif dengan unit organisasi yang berlaku dalam mengawasi hak akses informasi konsumen	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0877	Bekerja secara kooperatif dengan unit organisasi yang berlaku dalam mengawasi hak akses informasi konsumen	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0877	Bekerja secara kooperatif dengan unit organisasi yang berlaku dalam mengawasi hak akses informasi konsumen	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0877	Bekerja secara kooperatif dengan unit organisasi yang berlaku dalam mengawasi hak akses informasi konsumen	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0877	Bekerja secara kooperatif dengan unit organisasi yang berlaku dalam mengawasi hak akses informasi konsumen	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0935	Lakukan penilaian risiko keamanan informasi.	annual-risk-assessment-performed (pemeriksaan proses)	Lakukan penilaian risiko tahunan pada organisasi Anda. Penilaian risiko dapat membantu dalam menentukan kemungkinan dan dampak dari risiko dan/atau kerentanan yang diidentifikasi yang mempengaruhi suatu organisasi.
T0960	Memantau perubahan pada sistem dan lingkungan operasinya.	lambda-concurrency-check	Aturan ini memastikan bahwa batas tinggi dan rendah konkurensi fungsi Lambda ditetapkan. Ini dapat membantu dalam menyusun dasar jumlah permintaan yang dilayani oleh fungsi Anda pada waktu tertentu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0960	Memantau perubahan pada sistem dan lingkungan operasiny a.	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0960	Memantau perubahan pada sistem dan lingkungan operasiny a.	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberika n visibilitas terperinc i ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpan an Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitorin g mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0960	Memantau perubahan pada sistem dan lingkungan operasiny a.	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemelihar aan kapasitas dan ketersediaan yang memadai. Penyeimba ng beban secara berkala mengirimk an ping, mencoba koneksi, atau mengirim permintaa n untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0960	Memantau perubahan pada sistem dan lingkungan operasiny a.	beanstalk-enhanced -health-reporting- diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkin kan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakiba tkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentif ikasi dan mengident ifikasi kemungkin an penyebab untuk diselidiki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0960	Memantau perubahan pada sistem dan lingkungan operasiny a.	cloudwatch-alarm-a ction-check	Amazon CloudWatc h mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasark an pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActi onRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), (okActionRequired Config Default: False). Nilai sebenarnya harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0960	Memantau perubahan pada sistem dan lingkungan operasiny a.	dynamodb-throughpu t-limit-check	Aktifkan aturan ini untuk memastika n bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/ tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyarat an throughput Anda. Aturan ini menghasil kan peringatan ketika throughpu t mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentas e WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
T0960	Memantau perubahan pada sistem dan lingkungan operasiny a.	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.
T0992	Tentukan bagaimana hasil pemantauan berkelanjutan akan digunakan dalam otorisasi yang sedang berlangsung.	ec2- instance-profile-a ttached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirk an profil instans ke instans Anda dapat membantu pengelola an hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0992	Tentukan bagaimana hasil pemantauan berkelanjutan akan digunakan dalam otorisasi yang sedang berlangsung.	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0992	Tentukan bagaimana hasil pemantauan berkelanjutan akan digunakan dalam otorisasi yang sedang berlangsung.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0992	Tentukan bagaimana hasil pemantauan berkelanjutan akan digunakan dalam otorisasi yang sedang berlangsung.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0992	Tentukan bagaimana hasil pemantauan berkelanjutan akan digunakan dalam otorisasi yang sedang berlangsung.	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0992	Tentukan bagaimana hasil pemantauan berkelanjutan akan digunakan dalam otorisasi yang sedang berlangsung.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0992	Tentukan bagaimana hasil pemantauan berkelanjutan akan digunakan dalam otorisasi yang sedang berlangsung.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
T0992	Tentukan bagaimana hasil pemantauan berkelanjutan akan digunakan dalam otorisasi yang sedang berlangsung.	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0992	Tentukan bagaimana hasil pemantauan berkelanjutan akan digunakan dalam otorisasi yang sedang berlangsung.	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0992	Tentukan bagaimana hasil pemantauan berkelanjutan akan digunakan dalam otorisasi yang sedang berlangsung.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0992	Tentukan bagaimana hasil pemantauan berkelanjutan akan digunakan dalam otorisasi yang sedang berlangsung.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0992	Tentukan bagaimana hasil pemantauan berkelanjutan akan digunakan dalam otorisasi yang sedang berlangsung.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0992	Tentukan bagaimana hasil pemantauan berkelanjutan akan digunakan dalam otorisasi yang sedang berlangsung.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0992	Tentukan bagaimana hasil pemantauan berkelanjutan akan digunakan dalam otorisasi yang sedang berlangsung.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0992	Tentukan bagaimana hasil pemantauan berkelanjutan akan digunakan dalam otorisasi yang sedang berlangsung.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0992	Tentukan bagaimana hasil pemantauan berkelanjutan akan digunakan dalam otorisasi yang sedang berlangsung.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0992	Tentukan bagaimana hasil pemantauan berkelanjutan akan digunakan dalam otorisasi yang sedang berlangsung.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0992	Tentukan bagaimana hasil pemantauan berkelanjutan akan digunakan dalam otorisasi yang sedang berlangsung.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0992	Tentukan bagaimana hasil pemantauan berkelanjutan akan digunakan dalam otorisasi yang sedang berlangsung.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
T0992	Tentukan bagaimana hasil pemantauan berkelanjutan akan digunakan dalam otorisasi yang sedang berlangsung.	secretsmanager-rotation-enabled-check	Aturan ini memastikan AWS rahasia Secrets Manager telah diaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0993	Menetapkan alat pemantauan berkelanjutan dan teknologi proses kontrol akses dan prosedur.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
T0993	Menetapkan alat pemantauan berkelanjutan dan teknologi proses kontrol akses dan prosedur.	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0993	Menetapkan alat pemantauan berkelanjutan dan teknologi proses kontrol akses dan prosedur.	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi, pengembalian, dan pendelegasian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
T0993	Menetapkan alat pemantauan berkelanjutan dan teknologi proses kontrol akses dan prosedur.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0993	Menetapkan alat pemantauan berkelanjutan dan teknologi proses kontrol akses dan prosedur.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0993	Menetapkan alat pemantauan berkelanjutan dan teknologi proses kontrol akses dan prosedur.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0993	Menetapkan alat pemantauan berkelanjutan dan teknologi proses kontrol akses dan prosedur.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
T0993	Menetapkan alat pemantauan berkelanjutan dan teknologi proses kontrol akses dan prosedur.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0993	Menetapkan alat pemantauan berkelanjutan dan teknologi proses kontrol akses dan prosedur.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0993	Menetapkan alat pemantauan berkelanjutan dan teknologi proses kontrol akses dan prosedur.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0993	Menetapkan alat pemantauan berkelanjutan dan teknologi proses kontrol akses dan prosedur.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0993	Menetapkan alat pemantauan berkelanjutan dan teknologi proses kontrol akses dan prosedur.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0993	Menetapkan alat pemantauan berkelanjutan dan teknologi proses kontrol akses dan prosedur.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0993	Menetapkan alat pemantauan berkelanjutan dan teknologi proses kontrol akses dan prosedur.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
T0993	Menetapkan alat pemantauan berkelanjutan dan teknologi proses kontrol akses dan prosedur.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk NIST 800 181.

Praktik Terbaik Operasional untuk NIST 1800 25

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini menyediakan contoh pemetaan antara NIST 1800-25 dan aturan Config terkelola AWS . Masing-masing AWS Config berlaku untuk AWS sumber daya tertentu, dan berhubungan dengan satu atau lebih kontrol NIST 1800-25. Kontrol NIST 1800-25 dapat dikaitkan dengan beberapa aturan. AWS Config Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.AM-2	Platform dan aplikasi perangkat lunak dalam organisasi diinventarisasi	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.
ID.AM-2	Platform dan aplikasi perangkat lunak dalam organisasi diinventarisasi	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventari

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			s platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.
ID.AM-2	Platform dan aplikasi perangkat lunak dalam organisasi diinventarisasi	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.AM-2	Platform dan aplikasi perangkat lunak dalam organisasi diinventarisasi	terlampir eip	Aturan ini memastikan Elastic IPs dialokasikan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan. Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.
ID.AM-2	Platform dan aplikasi perangkat lunak dalam organisasi diinventarisasi	vpc-network-acl-unused-periksa	Aturan ini memastikan bahwa daftar kontrol akses jaringan Amazon Virtual Private Cloud (VPC) sedang digunakan. Pemantauan untuk daftar kontrol akses jaringan yang tidak digunakan dapat membantu inventaris dan pengelolaan lingkungan Anda yang akurat.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.RA-1	Kerentanan aset diidentifikasi dan didokumentasikan	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relational Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.RA-1	Kerentanan aset diidentifikasi dan didokumentasikan	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
ID.RA-1	Kerentanan aset diidentifikasi dan didokumentasikan	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.RA-1	Kerentanan aset diidentifikasi dan didokumentasikan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
PR.AC-1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk perangkat, pengguna, dan proses yang berwenang	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk perangkat, pengguna, dan proses yang berwenang	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk perangkat, pengguna, dan proses yang berwenang	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk perangkat, pengguna, dan proses yang berwenang	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk perangkat, pengguna, dan proses yang berwenang	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk perangkat, pengguna, dan proses yang berwenang	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk perangkat, pengguna, dan proses yang berwenang	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk perangkat, pengguna, dan proses yang berwenang	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk perangkat, pengguna, dan proses yang berwenang	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk perangkat, pengguna, dan proses yang berwenang	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk perangkat, pengguna, dan proses yang berwenang	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk perangkat, pengguna, dan proses yang berwenang	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk perangkat, pengguna, dan proses yang berwenang	secretsmanager-rotation-enabled-check	Aturan ini memastikan AWS rahasia Secrets Manager telah diaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan.
PR.AC-3	Akses jarak jauh dikelola.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
PR.AC-3	Akses jarak jauh dikelola.	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositor i data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
PR.AC-3	Akses jarak jauh dikelola.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.AC-3	Akses jarak jauh dikelola.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
PR.AC-3	Akses jarak jauh dikelola.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.
PR.AC-3	Akses jarak jauh dikelola.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
PR.AC-3	Akses jarak jauh dikelola.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	s3- account-level-publ ic-access -blok-per iodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
PR.AC-3	Akses jarak jauh dikelola.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
PR.AC-3	Akses jarak jauh dikelola.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
PR.AC-5	Integritas jaringan dilindungi (misalnya, segregasi jaringan, segmentasi jaringan)	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositor i data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSear ch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerluka n gateway internet, perangkat NAT, atau koneksi VPN.
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	s3- account-level-publ ic-access -blok-per iodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/ 0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-1	Data-at-rest dilindungi	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
PR.DS-1	Data-at-rest dilindungi	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-1	Data-at-rest dilindungi	s3- default-encryption -kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
PR.DS-1	Data-at-rest dilindungi	sagemaker-notebook -instance-kms-kunci- dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-1	Data-at-rest dilindungi	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
PR.DS-1	Data-at-rest dilindungi	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-1	Data-at-rest dilindungi	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
PR.DS-1	Data-at-rest dilindungi	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
PR.DS-1	Data-at-rest dilindungi	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-1	Data-at-rest dilindungi	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
PR.DS-1	Data-at-rest dilindungi	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-1	Data-at-rest dilindungi	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
PR.DS-1	Data-at-rest dilindungi	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-1	Data-at-rest dilindungi	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-1	Data-at-rest dilindungi	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
PR.DS-1	Data-at-rest dilindungi	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-1	Data-at-rest dilindungi	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
PR.DS-1	Data-at-rest dilindungi	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-2	Data-in-transit dilindungi	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-2	Data-in-transit dilindungi	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
PR.DS-2	Data-in-transit dilindungi	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-2	Data-in-transit dilindungi	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
PR.DS-2	Data-in-transit dilindungi	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-2	Data-in-transit dilindungi	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
PR.DS-2	Data-in-transit dilindungi	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-2	Data-in-transit dilindungi	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
PR.DS-2	Data-in-transit dilindungi	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-6	Mekanisme pemeriksaan integrita s digunakan untuk memverifikasi perangkat lunak, firmware, dan integrita s informasi	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-6	Mekanisme pemeriksaan integrita s digunakan untuk memverifikasi perangkat lunak, firmware, dan integrita s informasi	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-1	Konfigurasi dasar teknologi informasi/ sistem kontrol industri dibuat dan dipelihara dengan menggabungkan prinsip-prinsip keamanan (misalnya konsep fungsionalitas terkecil)	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-1	Konfigurasi dasar teknologi informasi/ sistem kontrol industri dibuat dan dipelihara dengan menggabun gkan prinsip-prinsip keamanan (misalnya konsep fungsionalitas terkecil)	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-1	Konfigurasi dasar teknologi informasi/ sistem kontrol industri dibuat dan dipelihara dengan menggabungkan prinsip-prinsip keamanan (misalnya konsep fungsionalitas terkecil)	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-1	Konfigurasi dasar teknologi informasi/ sistem kontrol industri dibuat dan dipelihara dengan menggabun gkan prinsip-prinsip keamanan (misalnya konsep fungsionalitas terkecil)	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.
PR.IP-1	Konfigurasi dasar teknologi informasi/ sistem kontrol industri dibuat dan dipelihara dengan menggabun gkan prinsip-prinsip keamanan (misalnya konsep fungsionalitas terkecil)	ec2- volume-inuse-check	Aturan ini memastika n bahwa volume Amazon Elastic Block Store yang dilampirk an ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentika n, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-1	Konfigurasi dasar teknologi informasi/ sistem kontrol industri dibuat dan dipelihara dengan menggabungkan prinsip-prinsip keamanan (misalnya konsep fungsionalitas terkecil)	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-3	Proses kontrol perubahan konfigurasi sudah ada	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-3	Proses kontrol perubahan konfigurasi sudah ada	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-4	Pencadangan informasi dilakukan, dipelihara, dan diuji	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-4	Pencadangan informasi dilakukan, dipelihara, dan diuji	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-4	Pencadangan informasi dilakukan, dipelihara, dan diuji	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-4	Pencadangan informasi dilakukan, dipelihara, dan diuji	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-4	Pencadangan informasi dilakukan, dipelihara, dan diuji	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk cluster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-4	Pencadangan informasi dilakukan, dipelihara, dan diuji	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-4	Pencadangan informasi dilakukan, dipelihara, dan diuji	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-4	Pencadangan informasi dilakukan, dipelihara, dan diuji	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-4	Pencadangan informasi dilakukan, dipelihara, dan diuji	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-4	Pencadangan informasi dilakukan, dipelihara, dan diuji	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-4	Pencadangan informasi dilakukan, dipelihara, dan diuji	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-9	Rencana respon (Incident Response and Business Continuity) dan rencana pemulihan (Incident Recovery dan Disaster Recovery) sudah ada dan dikelola.	response-plan-exists-maintained (Pemeriksaan Proses)	Memastikan rencana respons insiden dibuat, dipelihara, dan didistribusikan kepada personel yang bertanggung jawab. Memiliki rencana respons yang diperbarui dan didokumentasikan secara formal dapat membantu memastikan personel respons memahami peran, tanggung jawab, dan proses yang harus diikuti selama insiden.
PR.IP-10	Rencana respons dan pemulihan diuji.	response-plan-tested (Pemeriksaan Proses)	Pastikan respon Insiden dan rencana pemulihan diuji. Ini dapat membantu dalam memahami apakah rencana Anda akan efektif selama insiden dan jika ada celah atau pembaruan yang perlu ditangani.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-12	Rencana manajemen kerentanan dikembangkan dan diimplementasikan.	vuln-management-plan-exists (Pemeriksaan Proses)	Pastikan rencana manajemen kerentanan dikembangkan dan diimplementasikan untuk memiliki proses yang ditentukan secara formal untuk mengatasi kerentanan di lingkungan Anda. Ini dapat mencakup alat manajemen kerentanan, irama pemindaian lingkungan, peran dan tanggung jawab.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-12	Rencana manajemen kerentanan dikembangkan dan diimplementasikan	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-12	Rencana manajemen kerentanan dikembangkan dan diimplementasikan	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-12	Rencana manajemen kerentanan dikembangkan dan diimplementasikan	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.MA-2	Pemeliharaan aset organisasi secara jarak jauh disetujui, dicatat, dan dilakukan dengan cara yang mencegah akses yang tidak sah	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.MA-2	Pemeliharaan aset organisasi secara jarak jauh disetujui, dicatat, dan dilakukan dengan cara yang mencegah akses yang tidak sah	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-1	Jaringan komunikasi dan kontrol dilindungi	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	autoscaling-launch -config-public-ip- dinonaktifkan	Jika Anda mengonfig urasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	ec2- instance-profile-a ttached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirk an profil instans ke instans Anda dapat membantu pengelola an hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositor i data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	ssm-document-not-p ublic	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkin kan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspo s informasi tentang akun, sumber daya, dan proses internal Anda.
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSear ch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerluka n gateway internet, perangkat NAT, atau koneksi VPN.
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfigurasi sistem untuk hanya menyediakan kemampuan penting	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfigurasi sistem untuk hanya menyediakan kemampuan penting	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfigurasi sistem untuk hanya menyediakan kemampuan penting	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	sagemaker-notebook -no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurk an ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfig urasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-8	Pemindaian kerentanan dilakukan.	vuln-scans-performed (Pemeriksaan Proses)	Pastikan pemindaian kerentanan dilakukan sesuai dengan persyaratan kepatuhan Anda. Irama pemindaian, alat yang digunakan, dan penggunaan hasil harus ditentukan oleh organisasi Anda.
RS.MI-3	Kerentanan yang baru diidentifikasi dikurangi atau didokumentasikan sebagai risiko yang diterima.	vuln-mitigated-accepted (Pemeriksaan Proses)	Pastikan kerentanan yang baru diidentifikasi diperbaiki atau didokumentasikan sebagai risiko yang diterima. Layanan seperti AWS Security Hub, Amazon Guard Duty, Amazon Inspector, dan AWS Config dapat membantu mengidentifikasi kerentanan di lingkungan Anda. Kerentanan harus diperbaiki atau diterima sebagai risiko sesuai dengan persyaratan kepatuhan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RS.MI-3	Kerentanan yang baru diidentifikasi dikurangi atau didokumen tasikan sebagai risiko yang diterima	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk NIST 1800 25.

Praktik Terbaik Operasional untuk NIST CSF

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini menyediakan contoh pemetaan antara NIST Cyber Security Framework (CSF) dan aturan AWS Config terkelola. Setiap AWS Config aturan berlaku untuk AWS sumber daya tertentu, dan berhubungan dengan satu atau lebih kontrol CSF NIST. Kontrol CSF NIST dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-1	Dasar operasi jaringan dan aliran data yang diharapkan untuk pengguna dan sistem ditetapkan dan dikelola	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.
DE.AE-1	Dasar operasi jaringan dan aliran data yang diharapkan	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	untuk pengguna dan sistem ditetapkan dan dikelola		t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-1	Dasar operasi jaringan dan aliran data yang diharapkan untuk pengguna dan sistem ditetapkan dan dikelola	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
DE.AE-1	Dasar operasi jaringan dan aliran data yang diharapkan untuk pengguna dan sistem ditetapkan dan dikelola	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-1	Dasar operasi jaringan dan aliran data yang diharapkan untuk pengguna dan sistem ditetapkan dan dikelola	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
DE.AE-1	Dasar operasi jaringan dan aliran data yang diharapkan untuk pengguna dan sistem ditetapkan dan dikelola	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-1	Dasar operasi jaringan dan aliran data yang diharapkan untuk pengguna dan sistem ditetapkan dan dikelola	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
DE.AE-1	Dasar operasi jaringan dan aliran data yang diharapkan untuk pengguna dan sistem ditetapkan dan dikelola	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-1	Dasar operasi jaringan dan aliran data yang diharapkan untuk pengguna dan sistem ditetapkan dan dikelola	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
DE.AE-1	Dasar operasi jaringan dan aliran data yang diharapkan untuk pengguna dan sistem ditetapkan dan dikelola	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-1	Dasar operasi jaringan dan aliran data yang diharapkan untuk pengguna dan sistem ditetapkan dan dikelola	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-1	Dasar operasi jaringan dan aliran data yang diharapkan untuk pengguna dan sistem ditetapkan dan dikelola	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-1	Dasar operasi jaringan dan aliran data yang diharapkan untuk pengguna dan sistem ditetapkan dan dikelola	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-1	Dasar operasi jaringan dan aliran data yang diharapkan untuk pengguna dan sistem ditetapkan dan dikelola	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-1	Dasar operasi jaringan dan aliran data yang diharapkan untuk pengguna dan sistem ditetapkan dan dikelola	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-1	Dasar operasi jaringan dan aliran data yang diharapkan untuk pengguna dan sistem ditetapkan dan dikelola	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-1	Dasar operasi jaringan dan aliran data yang diharapkan untuk pengguna dan sistem ditetapkan dan dikelola	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-1	Dasar operasi jaringan dan aliran data yang diharapkan untuk pengguna dan sistem ditetapkan dan dikelola	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-2	Peristiwa yang terdeteksi dianalisis untuk memahami target dan metode serangan	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-2	Peristiwa yang terdeteksi dianalisis untuk memahami target dan metode serangan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-3	Data peristiwa dikumpulkan dan dikorelasikan dari berbagai sumber dan sensor	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-3	Data peristiwa dikumpulkan dan dikorelasikan dari berbagai sumber dan sensor	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-3	Data peristiwa dikumpulkan dan dikorelasikan dari berbagai sumber dan sensor	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-3	Data peristiwa dikumpulkan dan dikorelasikan dari berbagai sumber dan sensor	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
DE.AE-3	Data peristiwa dikumpulkan dan dikorelasikan dari berbagai sumber dan sensor	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-3	Data peristiwa dikumpulkan dan dikorelasikan dari berbagai sumber dan sensor	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
DE.AE-3	Data peristiwa dikumpulkan dan dikorelasikan dari berbagai sumber dan sensor	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-3	Data peristiwa dikumpulkan dan dikorelasikan dari berbagai sumber dan sensor	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
DE.AE-3	Data peristiwa dikumpulkan dan dikorelasikan dari berbagai sumber dan sensor	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-3	Data peristiwa dikumpulkan dan dikorelasikan dari berbagai sumber dan sensor	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-3	Data peristiwa dikumpulkan dan dikorelasikan dari berbagai sumber dan sensor	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-3	Data peristiwa dikumpulkan dan dikorelasikan dari berbagai sumber dan sensor	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-3	Data peristiwa dikumpulkan dan dikorelasikan dari berbagai sumber dan sensor	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-3	Data peristiwa dikumpulkan dan dikorelasikan dari berbagai sumber dan sensor	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
DE.AE-4	Dampak peristiwa ditentukan	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-4	Dampak peristiwa ditentukan	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-4	Dampak peristiwa ditentukan	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-4	Dampak peristiwa ditentukan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-4	Dampak peristiwa ditentukan	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-4	Dampak peristiwa ditentukan	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-4	Dampak peristiwa ditentukan	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.AE-4	Dampak peristiwa ditentukan	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-1	Jaringan dipantau untuk mendeteksi potensi peristiwa keamanan siber	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
DE.CM-1	Jaringan dipantau untuk mendeteksi potensi peristiwa keamanan siber	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-1	Jaringan dipantau untuk mendeteks i potensi peristiwa keamanan siber	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-1	Jaringan dipantau untuk mendeteks i potensi peristiwa keamanan siber	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-1	Jaringan dipantau untuk mendeteks i potensi peristiwa keamanan siber	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-1	Jaringan dipantau untuk mendeteksi potensi peristiwa keamanan siber	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-1	Jaringan dipantau untuk mendeteksi potensi peristiwa keamanan siber	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-1	Jaringan dipantau untuk mendeteks i potensi peristiwa keamanan siber	s3- event-notification s-enabled	Pemberitahuan peristiwa Amazon S3 dapat memberi tahu personel terkait tentang modifikasi yang tidak disengaja atau disengaja pada objek bucket Anda. Contoh peringatan meliputi: objek baru adalah pembuatan, penghapusan objek, restorasi objek, objek yang hilang dan direplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-1	Jaringan dipantau untuk mendeteks i potensi peristiwa keamanan siber	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-1	Jaringan dipantau untuk mendeteks i potensi peristiwa keamanan siber	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
DE.CM-3	Aktivitas personel dipantau untuk mendeteksi potensi peristiwa keamanan siber	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteks i aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-3	Aktivitas personel dipantau untuk mendeteksi potensi peristiwa keamanan siber	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-3	Aktivitas personel dipantau untuk mendeteksi potensi peristiwa keamanan siber	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-3	Aktivitas personel dipantau untuk mendeteksi potensi peristiwa keamanan siber	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-3	Aktivitas personel dipantau untuk mendeteksi potensi peristiwa keamanan siber	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-3	Aktivitas personel dipantau untuk mendeteksi potensi peristiwa keamanan siber	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-4	Kode berbahaya terdeteksi	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-4	Kode berbahaya terdeteksi	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-5	Kode seluler yang tidak sah terdeteksi	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.
DE.CM-5	Kode seluler yang tidak sah terdeteksi	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-5	Kode seluler yang tidak sah terdeteksi	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-5	Kode seluler yang tidak sah terdeteksi	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-5	Kode seluler yang tidak sah terdeteksi	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-5	Kode seluler yang tidak sah terdeteksi	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-6	Aktivitas penyedia layanan eksternal dipantau untuk mendeteksi potensi peristiwa keamanan siber	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
DE.CM-6	Aktivitas penyedia layanan eksternal dipantau untuk mendeteksi potensi peristiwa keamanan siber	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-6	Aktivitas penyedia layanan eksternal dipantau untuk mendeteksi potensi peristiwa keamanan siber	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-6	Aktivitas penyedia layanan eksternal dipantau untuk mendeteksi potensi peristiwa keamanan siber	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-6	Aktivitas penyedia layanan eksternal dipantau untuk mendeteksi potensi peristiwa keamanan siber	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-6	Aktivitas penyedia layanan eksternal dipantau untuk mendeteksi potensi peristiwa keamanan siber	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-7	Pemantauan untuk personel, koneksi, perangkat, dan perangkat lunak yang tidak sah dilakukan	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
DE.CM-7	Pemantauan untuk personel, koneksi, perangkat, dan perangkat lunak yang tidak sah dilakukan	cloudtrail-s3-dataevents-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-7	Pemantauan untuk personel, koneksi, perangkat, dan perangkat lunak yang tidak sah dilakukan	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-7	Pemantauan untuk personel, koneksi, perangkat, dan perangkat lunak yang tidak sah dilakukan	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-7	Pemantauan untuk personel, koneksi, perangkat, dan perangkat lunak yang tidak sah dilakukan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-7	Pemantauan untuk personel, koneksi, perangkat, dan perangkat lunak yang tidak sah dilakukan	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-7	Pemantauan untuk personel, koneksi, perangkat, dan perangkat lunak yang tidak sah dilakukan	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-7	Pemantauan untuk personel, koneksi, perangkat, dan perangkat lunak yang tidak sah dilakukan	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.CM-7	Pemantauan untuk personel, koneksi, perangkat, dan perangkat lunak yang tidak sah dilakukan	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.DP-4	Informasi deteksi peristiwa dikomunik asikan	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.
DE.DP-4	Informasi deteksi peristiwa dikomunik asikan	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.DP-4	Informasi deteksi peristiwa dikomunik asikan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.DP-4	Informasi deteksi peristiwa dikomunikasikan	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.DP-4	Informasi deteksi peristiwa dikomunik asikan	s3- event-notification s-enabled	Pemberitahuan peristiwa Amazon S3 dapat memberi tahu personel terkait tentang modifikasi yang tidak disengaja atau disengaja pada objek bucket Anda. Contoh peringatan meliputi: objek baru adalah pembuatan, penghapusan objek, restorasi objek, objek yang hilang dan direplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.DP-4	Informasi deteksi peristiwa dikomunik asikan	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.DP-4	Informasi deteksi peristiwa dikomunikasikan	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
DE.DP-5	Proses deteksi terus ditingkatkan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.AM-2	Platform dan aplikasi perangkat lunak dalam organisasi diinventarisasi	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.AM-2	Platform dan aplikasi perangkat lunak dalam organisasi diinventarisasi	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.AM-2	Platform dan aplikasi perangkat lunak dalam organisasi diinventarisasi	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.
ID.AM-2	Platform dan aplikasi perangkat lunak dalam organisasi diinventarisasi	terlampir eip	Aturan ini memastikan Elastic IPs dialokasikan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan. Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.AM-2	Platform dan aplikasi perangkat lunak dalam organisasi diinventarisasi	vpc-network-acl-unused-periksa	Aturan ini memastikan bahwa daftar kontrol akses jaringan Amazon Virtual Private Cloud (VPC) sedang digunakan. Pemantauan untuk daftar kontrol akses jaringan yang tidak digunakan dapat membantu inventaris dan pengelolaan lingkungan Anda yang akurat.
ID.AM-3	Komunikasi organisasi dan aliran data dipetakan	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.AM-3	Komunikasi organisasi dan aliran data dipetakan	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.AM-3	Komunikasi organisasi dan aliran data dipetakan	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.AM-3	Komunikasi organisasi dan aliran data dipetakan	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.AM-3	Komunikasi organisasi dan aliran data dipetakan	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.AM-3	Komunikasi organisasi dan aliran data dipetakan	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.AM-3	Komunikasi organisasi dan aliran data dipetakan	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.BE-5	Persyaratan ketahanan untuk mendukung pengiriman layanan kritis ditetapkan untuk semua negara operasi (misalnya di bawah paksaan/serangan, selama pemulihan, operasi normal)	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.BE-5	Persyaratan ketahanan untuk mendukung pengiriman layanan kritis ditetapkan untuk semua negara operasi (misalnya di bawah paksaan/serangan, selama pemulihan, operasi normal)	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.BE-5	Persyaratan ketahanan untuk mendukung pengiriman layanan kritis ditetapkan untuk semua negara operasi (misalnya di bawah paksaan/serangan, selama pemulihan, operasi normal)	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.BE-5	Persyaratan ketahanan untuk mendukung pengiriman layanan kritis ditetapkan untuk semua negara operasi (misalnya di bawah paksaan/serangan, selama pemulihan, operasi normal)	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.BE-5	Persyaratan ketahanan untuk mendukung pengiriman layanan kritis ditetapkan untuk semua negara operasi (misalnya di bawah paksaan/serangan, selama pemulihan, operasi normal)	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.BE-5	Persyaratan ketahanan untuk mendukung pengirima n layanan kritis ditetapkan untuk semua negara operasi (misalnya di bawah paksaan/serangan, selama pemulihan, operasi normal)	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.BE-5	Persyaratan ketahanan untuk mendukung pengiriman layanan kritis ditetapkan untuk semua negara operasi (misalnya di bawah paksaan/serangan, selama pemulihan, operasi normal)	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.BE-5	Persyaratan ketahanan untuk mendukung pengiriman layanan kritis ditetapkan untuk semua negara operasi (misalnya di bawah paksaan/serangan, selama pemulihan, operasi normal)	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.BE-5	Persyaratan ketahanan untuk mendukung pengiriman layanan kritis ditetapkan untuk semua negara operasi (misalnya di bawah paksaan/serangan, selama pemulihan, operasi normal)	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.BE-5	Persyaratan ketahanan untuk mendukung pengiriman layanan kritis ditetapkan untuk semua negara operasi (misalnya di bawah paksaan/serangan, selama pemulihan, operasi normal)	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.BE-5	Persyaratan ketahanan untuk mendukung pengiriman layanan kritis ditetapkan untuk semua negara operasi (misalnya di bawah paksaan/serangan, selama pemulihan, operasi normal)	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.BE-5	Persyaratan ketahanan untuk mendukung pengiriman layanan kritis ditetapkan untuk semua negara operasi (misalnya di bawah paksaan/serangan, selama pemulihan, operasi normal)	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.BE-5	Persyaratan ketahanan untuk mendukung pengiriman layanan kritis ditetapkan untuk semua negara operasi (misalnya di bawah paksaan/serangan, selama pemulihan, operasi normal)	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.BE-5	Persyaratan ketahanan untuk mendukung pengiriman layanan kritis ditetapkan untuk semua negara operasi (misalnya di bawah paksaan/serangan, selama pemulihan, operasi normal)	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.BE-5	Persyaratan ketahanan untuk mendukung pengirima n layanan kritis ditetapkan untuk semua negara operasi (misalnya di bawah paksaan/serangan, selama pemulihan, operasi normal)	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.BE-5	Persyaratan ketahanan untuk mendukung pengirima n layanan kritis ditetapkan untuk semua negara operasi (misalnya di bawah paksaan/serangan, selama pemulihan, operasi normal)	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimpleme ntasikan untuk mencapai persyarat an ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivi tas jika salah satu koneksi Site-to-S ite VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivi tas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.RA-1	Kerentanan aset diidentifikasi dan didokumentasikan	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relational Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.RA-1	Kerentanan aset diidentifikasi dan didokumentasikan	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
ID.RA-1	Kerentanan aset diidentifikasi dan didokumentasikan	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.RA-1	Kerentanan aset diidentifikasi dan didokumentasikan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.RA-2	Intelijen ancaman cyber diterima dari forum dan sumber berbagi informasi	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.RA-3	Ancaman, baik internal maupun eksternal, diidentif ikasi dan didokumen tasikan	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.RA-3	Ancaman, baik internal maupun eksternal, diidentif ikasi dan didokumen tasikan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
ID.RA-5	Ancaman, kerentana n, kemungkinan, dan dampak digunakan untuk menentukan risiko	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.RA-5	Ancaman, kerentanan, kemungkinan, dan dampak digunakan untuk menentukan risiko	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.RA-5	Ancaman, kerentanan, kemungkinan, dan dampak digunakan untuk menentukan risiko	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.RA-5	Ancaman, kerentanan, kemungkinan, dan dampak digunakan untuk menentukan risiko	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.SC-4	Pemasok dan mitra pihak ketiga secara rutin dinilai menggunakan audit, hasil pengujian, atau bentuk evaluasi lainnya untuk mengonfirmasi bahwa mereka memenuhi kewajiban kontrak mereka.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
ID.SC-4	Pemasok dan mitra pihak ketiga secara rutin dinilai menggunakan audit, hasil pengujian, atau bentuk evaluasi lainnya untuk mengonfirmasi bahwa mereka memenuhi kewajiban kontrak mereka.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.SC-4	Pemasok dan mitra pihak ketiga secara rutin dinilai menggunakan audit, hasil pengujian, atau bentuk evaluasi lainnya untuk mengonfirmasi bahwa mereka memenuhi kewajiban kontrak mereka.	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.SC-4	Pemasok dan mitra pihak ketiga secara rutin dinilai menggunakan audit, hasil pengujian, atau bentuk evaluasi lainnya untuk mengonfirmasi bahwa mereka memenuhi kewajiban kontrak mereka.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk perangkat, pengguna, dan proses yang berwenang	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.
PR.AC-1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk perangkat, pengguna, dan proses yang berwenang	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk perangkat, pengguna, dan proses yang berwenang	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk perangkat, pengguna, dan proses yang berwenang	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk perangkat, pengguna, dan proses yang berwenang	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk perangkat, pengguna, dan proses yang berwenang	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk perangkat, pengguna, dan proses yang berwenang	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk perangkat, pengguna, dan proses yang berwenang	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk perangkat, pengguna, dan proses yang berwenang	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk perangkat, pengguna, dan proses yang berwenang	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk perangkat, pengguna, dan proses yang berwenang	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk perangkat, pengguna, dan proses yang berwenang	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsageUsia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk perangkat, pengguna, dan proses yang berwenang	secretsmanager-rotation-enabled-check	Aturan ini memastikan AWS rahasia Secrets Manager telah diaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk perangkat, pengguna, dan proses yang berwenang	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
PR.AC-3	Akses jarak jauh dikelola.	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositor i data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
PR.AC-3	Akses jarak jauh dikelola.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.AC-3	Akses jarak jauh dikelola.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
PR.AC-3	Akses jarak jauh dikelola.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.
PR.AC-3	Akses jarak jauh dikelola.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
PR.AC-3	Akses jarak jauh dikelola.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	s3- account-level-publ ic-access -blok-per iodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
PR.AC-3	Akses jarak jauh dikelola.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
PR.AC-3	Akses jarak jauh dikelola.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-3	Akses jarak jauh dikelola.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsageUsia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
PR.AC-4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa yang paling rendah dan pemisahan tugas	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositor i data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSear ch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerluka n gateway internet, perangkat NAT, atau koneksi VPN.
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	s3- account-level-publ ic-access -blok-per iodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan)	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/ 0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-6	Identitas dibuktikan dan terikat pada kredensi dan ditegaskan dalam interaksi	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktifkan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediakan sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-6	Identitas dibuktikan dan terikat pada kredensi dan ditegaskan dalam interaksi	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-7	Pengguna, perangkat, dan aset lainnya diautentikasi (misalnya, faktor tunggal, multi-faktor) yang sepadan dengan risiko transaksi (misalnya, risiko keamanan dan privasi individu dan risiko organisasi lainnya)	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-7	Pengguna, perangkat , dan aset lainnya diautentikasi (misalnya, faktor tunggal, multi-faktor) yang sepadan dengan risiko transaksi (misalnya, risiko keamanan dan privasi individu dan risiko organisasi lainnya)	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastika n otentikasi multi-fak tor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-7	Pengguna, perangkat, dan aset lainnya diautentikasi (misalnya, faktor tunggal, multi-faktor) yang sepadan dengan risiko transaksi (misalnya, risiko keamanan dan privasi individu dan risiko organisasi lainnya)	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-7	Pengguna, perangkat, dan aset lainnya diautentikasi (misalnya, faktor tunggal, multi-faktor) yang sepadan dengan risiko transaksi (misalnya, risiko keamanan dan privasi individu dan risiko organisasi lainnya)	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-7	Pengguna, perangkat, dan aset lainnya diautentikasi (misalnya, faktor tunggal, multi-faktor) yang sepadan dengan risiko transaksi (misalnya, risiko keamanan dan privasi individu dan risiko organisasi lainnya)	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
PR.AT-1	Semua pengguna diinformasikan dan dilatih	security-awareness-program-exists (pemeriksaan proses)	Membangun dan memelihara program kesadaran keamanan untuk organisasi Anda. Program kesadaran keamanan mendidik karyawan tentang cara melindungi organisasi mereka dari berbagai pelanggaran atau insiden keamanan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-1	Data-at-rest dilindungi	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
PR.DS-1	Data-at-rest dilindungi	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-1	Data-at-rest dilindungi	s3- default-encryption -kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
PR.DS-1	Data-at-rest dilindungi	sagemaker-notebook -instance-kms-kunci- dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-1	Data-at-rest dilindungi	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
PR.DS-1	Data-at-rest dilindungi	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-1	Data-at-rest dilindungi	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
PR.DS-1	Data-at-rest dilindungi	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
PR.DS-1	Data-at-rest dilindungi	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-1	Data-at-rest dilindungi	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
PR.DS-1	Data-at-rest dilindungi	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-1	Data-at-rest dilindungi	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
PR.DS-1	Data-at-rest dilindungi	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-1	Data-at-rest dilindungi	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-1	Data-at-rest dilindungi	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
PR.DS-1	Data-at-rest dilindungi	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-1	Data-at-rest dilindungi	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
PR.DS-1	Data-at-rest dilindungi	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-2	Data-in-transit dilindungi	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-2	Data-in-transit dilindungi	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
PR.DS-2	Data-in-transit dilindungi	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-2	Data-in-transit dilindungi	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
PR.DS-2	Data-in-transit dilindungi	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-2	Data-in-transit dilindungi	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
PR.DS-2	Data-in-transit dilindungi	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-2	Data-in-transit dilindungi	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
PR.DS-2	Data-in-transit dilindungi	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-3	Aset dikelola secara formal selama penghapusan, transfer, dan disposisi	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-3	Aset dikelola secara formal selama penghapusan, transfer, dan disposisi	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-3	Aset dikelola secara formal selama penghapusan, transfer, dan disposisi	terlampir eip	Aturan ini memastikan Elastic IPs dialokasikan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan. Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-4	Kapasitas yang memadai untuk memastikan ketersedi aan tetap terjaga	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-4	Kapasitas yang memadai untuk memastikan ketersedi aan tetap terjaga	efs-in-backup-plan	Untuk membantu proses pencadang an data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-4	Kapasitas yang memadai untuk memastikan ketersedi aan tetap terjaga	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-4	Kapasitas yang memadai untuk memastikan ketersedi aan tetap terjaga	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) menyediakan ketersediaan dan daya tahan yang ditingkatkan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-4	Kapasitas yang memadai untuk memastikan ketersedi aan tetap terjaga	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-4	Kapasitas yang memadai untuk memastikan ketersedi aan tetap terjaga	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-4	Kapasitas yang memadai untuk memastikan ketersedi aan tetap terjaga	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimpleme ntasikan untuk mencapai persyarat an ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivi tas jika salah satu koneksi Site-to-S ite VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivi tas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-5	Perlindungan terhadap kebocoran data diimpleme ntasikan	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfig urasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-5	Perlindungan terhadap kebocoran data diimpleme ntasikan	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-5	Perlindungan terhadap kebocoran data diimpleme ntasikan	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-5	Perlindungan terhadap kebocoran data diimplementasikan	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
PR.DS-5	Perlindungan terhadap kebocoran data diimplementasikan	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-5	Perlindungan terhadap kebocoran data diimpleme ntasikan	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteks i aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
PR.DS-5	Perlindungan terhadap kebocoran data diimpleme ntasikan	codebuild-project-envvar-awscred-per iksa	Pastikan kredensi otentikasi AWS_ACCES S_KEY_ID dan AWS_SECRE T_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild . Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabk an paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-5	Perlindungan terhadap kebocoran data diimpleme ntasikan	codebuild-project-source-repo-url-pe riksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredenal masuk dalam lingkungan proyek Codebuild . AWS Gunakan OAuth alih-alih token akses pribadi atau kredensyal masuk untuk memberika n otorisasi untuk mengakses GitHub atau repositori Bitbucket.
PR.DS-5	Perlindungan terhadap kebocoran data diimpleme ntasikan	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-5	Perlindungan terhadap kebocoran data diimpleme ntasikan	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.DS-5	Perlindungan terhadap kebocoran data diimpleme ntasikan	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSear ch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerluka n gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-5	Perlindungan terhadap kebocoran data diimpleme ntasikan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
PR.DS-5	Perlindungan terhadap kebocoran data diimpleme ntasikan	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-5	Perlindungan terhadap kebocoran data diimpleme ntasikan	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-5	Perlindungan terhadap kebocoran data diimpleme ntasikan	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
PR.DS-5	Perlindungan terhadap kebocoran data diimpleme ntasikan	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-5	Perlindungan terhadap kebocoran data diimpleme ntasikan	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-5	Perlindungan terhadap kebocoran data diimpleme ntasikan	s3- account-level-publ ic-access -blok-per iodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-5	Perlindungan terhadap kebocoran data diimpleme ntasikan	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediak an metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinc i untuk permintaa n yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-5	Perlindungan terhadap kebocoran data diimpleme ntasikan	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
PR.DS-5	Perlindungan terhadap kebocoran data diimpleme ntasikan	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-5	Perlindungan terhadap kebocoran data diimpleme ntasikan	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
PR.DS-5	Perlindungan terhadap kebocoran data diimpleme ntasikan	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-6	Mekanisme pemeriksaan integrita s digunakan untuk memverifikasi perangkat lunak, firmware, dan integrita s informasi	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-6	Mekanisme pemeriksaan integrita s digunakan untuk memverifikasi perangkat lunak, firmware, dan integrita s informasi	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-7	Lingkungan pengembangan dan pengujian terpisah dari lingkungan produksi	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-7	Lingkungan pengembangan dan pengujian terpisah dari lingkungan produksi	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-7	Lingkungan pengembangan dan pengujian terpisah dari lingkungan produksi	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.
PR.DS-7	Lingkungan pengembangan dan pengujian terpisah dari lingkungan produksi	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-7	Lingkungan pengembangan dan pengujian terpisah dari lingkungan produksi	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-7	Lingkungan pengembangan dan pengujian terpisah dari lingkungan produksi	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-1	Konfigurasi dasar teknologi informasi/ sistem kontrol industri dibuat dan dipelihara dengan menggabungkan prinsip-prinsip keamanan (misalnya konsep fungsionalitas terkecil)	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-1	Konfigurasi dasar teknologi informasi/ sistem kontrol industri dibuat dan dipelihara dengan menggabun gkan prinsip-prinsip keamanan (misalnya konsep fungsionalitas terkecil)	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-1	Konfigurasi dasar teknologi informasi/ sistem kontrol industri dibuat dan dipelihara dengan menggabungkan prinsip-prinsip keamanan (misalnya konsep fungsionalitas terkecil)	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-1	Konfigurasi dasar teknologi informasi/ sistem kontrol industri dibuat dan dipelihara dengan menggabun gkan prinsip-prinsip keamanan (misalnya konsep fungsionalitas terkecil)	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.
PR.IP-1	Konfigurasi dasar teknologi informasi/ sistem kontrol industri dibuat dan dipelihara dengan menggabun gkan prinsip-prinsip keamanan (misalnya konsep fungsionalitas terkecil)	ec2- volume-inuse-check	Aturan ini memastika n bahwa volume Amazon Elastic Block Store yang dilampirk an ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentika n, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-1	Konfigurasi dasar teknologi informasi/ sistem kontrol industri dibuat dan dipelihara dengan menggabungkan prinsip-prinsip keamanan (misalnya konsep fungsionalitas terkecil)	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-2	Siklus Hidup Pengembangan Sistem untuk mengelola sistem diimplementasikan	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild . Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-2	Siklus Hidup Pengembangan Sistem untuk mengelola sistem diimplementasikan	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber GitHub atau Bitbucket tidak berisi token akses pribadi, kredenal masuk dalam lingkungan proyek Codebuild . AWS Gunakan OAuth alih-alih token akses pribadi atau kredensyal masuk untuk memberikan otorisasi untuk mengakses GitHub atau repositori Bitbucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-2	Siklus Hidup Pengembangan Sistem untuk mengelola sistem diimplementasikan	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-3	Proses kontrol perubahan konfigurasi sudah ada	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-3	Proses kontrol perubahan konfigurasi sudah ada	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-4	Pencadangan informasi dilakukan, dipelihara, dan diuji	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-4	Pencadangan informasi dilakukan, dipelihara, dan diuji	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-4	Pencadangan informasi dilakukan, dipelihara, dan diuji	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-4	Pencadangan informasi dilakukan, dipelihara, dan diuji	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-4	Pencadangan informasi dilakukan, dipelihara, dan diuji	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-4	Pencadangan informasi dilakukan, dipelihara, dan diuji	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-4	Pencadangan informasi dilakukan, dipelihara, dan diuji	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-4	Pencadangan informasi dilakukan, dipelihara, dan diuji	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-4	Pencadangan informasi dilakukan, dipelihara, dan diuji	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-4	Pencadangan informasi dilakukan, dipelihara, dan diuji	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-4	Pencadangan informasi dilakukan, dipelihara, dan diuji	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-7	Proses perlindungan ditingkatkan	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.
PR.IP-8	Efektivitas teknologi perlindungan dibagi	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-8	Efektivitas teknologi perlindungan dibagi	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.IP-8	Efektivitas teknologi perlindungan dibagi	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-8	Efektivitas teknologi perlindungan dibagi	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.IP-8	Efektivitas teknologi perlindungan dibagi	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-8	Efektivitas teknologi perlindungan dibagi	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
PR.IP-8	Efektivitas teknologi perlindungan dibagi	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-8	Efektivitas teknologi perlindungan dibagi	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.IP-8	Efektivitas teknologi perlindungan dibagi	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-8	Efektivitas teknologi perlindungan dibagi	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
PR.IP-8	Efektivitas teknologi perlindungan dibagi	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-8	Efektivitas teknologi perlindungan dibagi	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-12	Rencana manajemen kerentanan dikembangkan dan diimplementasikan	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-12	Rencana manajemen kerentanan dikembangkan dan diimplementasikan	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.IP-12	Rencana manajemen kerentanan dikembangkan dan diimplementasikan	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.MA-2	Pemeliharaan aset organisasi secara jarak jauh disetujui, dicatat, dan dilakukan dengan cara yang mencegah akses yang tidak sah	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.MA-2	Pemeliharaan aset organisasi secara jarak jauh disetujui, dicatat, dan dilakukan dengan cara yang mencegah akses yang tidak sah	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-1	Jaringan komunikasi dan kontrol dilindungi	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-1	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	autoscaling-launch -config-public-ip- dinonaktifkan	Jika Anda mengonfig urasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	ec2- instance-profile-a ttached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirk an profil instans ke instans Anda dapat membantu pengelola an hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositor i data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	ssm-document-not-p ublic	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkin kan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspo s informasi tentang akun, sumber daya, dan proses internal Anda.
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSear ch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerluka n gateway internet, perangkat NAT, atau koneksi VPN.
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfigurasi sistem untuk hanya menyediakan kemampuan penting	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfigurasi sistem untuk hanya menyediakan kemampuan penting	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfigurasi sistem untuk hanya menyediakan kemampuan penting	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	sagemaker-notebook -no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
PR.PT-3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurk an ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-4	Jaringan komunikasi dan kontrol dilindungi	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-5	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan	dynamodb-in-backup-plan	Untuk membantu proses pencadang an data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-5	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-5	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan	efs-in-backup-plan	Untuk membantu proses pencadang an data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-5	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan	elb-cross-zone-loa d-menyeimbangkan diaktifkan	Aktifkan penyeimba ngan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimba ngan beban lintas zona mengurang i kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkat kan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-5	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relationa l Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindun gan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersedi aan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-5	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-5	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan	redshift-backup-en abled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifka n untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-5	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemelihar aan kapasitas dan ketersediaan yang memadai. Penyeimba ng beban secara berkala mengirimk an ping, mencoba koneksi, atau mengirim permintaa n untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-5	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-5	Mekanisme (misalnya, failsafe, load balancing, hot swap) diterapkan untuk mencapai persyaratan ketahanan dalam situasi normal dan merugikan	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-5	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan	dynamodb-pitr-enab led	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertah ankan cadangan dengan memastika n bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-5	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-5	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan	elb-deletion-prote ction-enabled	Aturan ini memastika n bahwa Elastic Load Balancing memiliki perlindun gan penghapus an yang diaktifka n. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersedi aan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-5	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) menyediakan ketersediaan dan daya tahan yang ditingkatkan untuk instans database. Saat Anda menyediak an instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastru ktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutk an operasi database

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			segera setelah failover selesai.
PR.PT-5	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-5	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-5	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimpleme ntasikan untuk mencapai persyarat an ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivi tas jika salah satu koneksi Site-to-S ite VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivi tas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RC.RP-1	Rencana pemulihan dijalankan selama atau setelah insiden keamanan siber	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RC.RP-1	Rencana pemulihan dijalankan selama atau setelah insiden keamanan siber	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RC.RP-1	Rencana pemulihan dijalankan selama atau setelah insiden keamanan siber	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RC.RP-1	Rencana pemulihan dijalankan selama atau setelah insiden keamanan siber	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RC.RP-1	Rencana pemulihan dijalankan selama atau setelah insiden keamanan siber	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RC.RP-1	Rencana pemulihan dijalankan selama atau setelah insiden keamanan siber	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RC.RP-1	Rencana pemulihan dijalankan selama atau setelah insiden keamanan siber	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RC.RP-1	Rencana pemulihan dijalankan selama atau setelah insiden keamanan siber	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RC.RP-1	Rencana pemulihan dijalankan selama atau setelah insiden keamanan siber	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RC.RP-1	Rencana pemulihan dijalankan selama atau setelah insiden keamanan siber	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RC.RP-1	Rencana pemulihan dijalankan selama atau setelah insiden keamanan siber	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RC.RP-1	Rencana pemulihan dijalankan selama atau setelah insiden keamanan siber	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RC.RP-1	Rencana pemulihan dijalankan selama atau setelah insiden keamanan siber	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) menyediakan ketersediaan dan daya tahan yang ditingkatkan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			segera setelah failover selesai.
RC.RP-1	Rencana pemulihan dijalankan selama atau setelah insiden keamanan siber	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RC.RP-1	Rencana pemulihan dijalankan selama atau setelah insiden keamanan siber	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RC.RP-1	Rencana pemulihan dijalankan selama atau setelah insiden keamanan siber	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RS.AN-2	Dampak dari insiden tersebut dipahami	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RS.MI-3	Kerentanan yang baru diidentifikasi dikurangi atau didokumen tasikan sebagai risiko yang diterima	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RS.RP-1	Rencana respons dijalankan selama atau setelah insiden	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RS.RP-1	Rencana respons dijalankan selama atau setelah insiden	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup Anda diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RS.RP-1	Rencana respons dijalankan selama atau setelah insiden	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
RS.RP-1	Rencana respons dijalankan selama atau setelah insiden	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RS.RP-1	Rencana respons dijalankan selama atau setelah insiden	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RS.RP-1	Rencana respons dijalankan selama atau setelah insiden	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RS.RP-1	Rencana respons dijalankan selama atau setelah insiden	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RS.RP-1	Rencana respons dijalankan selama atau setelah insiden	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RS.RP-1	Rencana respons dijalankan selama atau setelah insiden	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RS.RP-1	Rencana respons dijalankan selama atau setelah insiden	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RS.RP-1	Rencana respons dijalankan selama atau setelah insiden	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RS.RP-1	Rencana respons dijalankan selama atau setelah insiden	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RS.RP-1	Rencana respons dijalankan selama atau setelah insiden	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RS.RP-1	Rencana respons dijalankan selama atau setelah insiden	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RS.RP-1	Rencana respons dijalankan selama atau setelah insiden	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RS.RP-1	Rencana respons dijalankan selama atau setelah insiden	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) menyediakan ketersediaan dan daya tahan yang ditingkatkan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			segera setelah failover selesai.
RS.RP-1	Rencana respons dijalankan selama atau setelah insiden	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RS.RP-1	Rencana respons dijalankan selama atau setelah insiden	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RS.RP-1	Rencana respons dijalankan selama atau setelah insiden	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
RS.RP-1	Rencana respons dijalankan selama atau setelah insiden	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk NIST CSF.

Praktik Terbaik Operasional untuk Kerangka Privasi NIST v1.0

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini menyediakan contoh pemetaan antara Kerangka Privasi NIST dan aturan AWS Config terkelola. Setiap AWS Config aturan berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau lebih kontrol Kerangka Privasi NIST. Kontrol Kerangka Privasi NIST dapat dikaitkan dengan beberapa AWS Config aturan. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CT.DM-P7	Mekanisme untuk mentransmisikan izin pemrosesan dan nilai data terkait dengan elemen data ditetapkan dan di tempat.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
CT.DM-P7	Mekanisme untuk mentransmisikan izin pemrosesan dan nilai	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	data terkait dengan elemen data ditetapkan dan di tempat.		dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.
CT.DM-P7	Mekanisme untuk mentransmisikan izin pemrosesan dan nilai data terkait dengan elemen data ditetapkan dan di tempat.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CT.DM-P7	Mekanisme untuk mentransmisikan izin pemrosesan dan nilai data terkait dengan elemen data ditetapkan dan di tempat.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CT.DM-P7	Mekanisme untuk mentransmisikan izin pemrosesan dan nilai data terkait dengan elemen data ditetapkan dan di tempat.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CT.DM-P7	Mekanisme untuk mentransmisikan izin pemrosesan dan nilai data terkait dengan elemen data ditetapkan dan di tempat.	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
CT.DM-P7	Mekanisme untuk mentransmisikan izin pemrosesan dan nilai data terkait dengan elemen data ditetapkan dan di tempat.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CT.DM-P7	Mekanisme untuk mentransmisikan izin pemrosesan dan nilai data terkait dengan elemen data ditetapkan dan di tempat.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
CT.DM-P7	Mekanisme untuk mentransmisikan izin pemrosesan dan nilai data terkait dengan elemen data ditetapkan dan di tempat.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CT.DM-P8	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan dan menggabungkan prinsip minimalisasi data.	audit-log-policy-exists(Pemeriksaan Proses)	Menetapkan dan memelihara kebijakan manajemen log audit yang menentukan persyaratan pencatatan organisasi Anda. Ini termasuk, namun tidak terbatas pada, peninjauan dan retensi log audit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CT.DM-P8	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan dan menggabungkan prinsip minimalisasi data.	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CT.DM-P8	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan dan menggabungkan prinsip minimalisasi data.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
CT.DM-P8	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan dan menggabungkan prinsip minimalisasi data.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CT.DM-P8	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan dan menggabungkan prinsip minimalisasi data.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
CT.DM-P8	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan dan menggabungkan prinsip minimalisasi data.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CT.DM-P8	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan dan menggabungkan prinsip minimalisasi data.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CT.DM-P8	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan dan menggabungkan prinsip minimalisasi data.	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CT.DM-P8	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan dan menggabungkan prinsip minimalisasi data.	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/ tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
CT.DM-P8	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan dan menggabungkan prinsip minimalisasi data.	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CT.DM-P8	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan dan menggabungkan prinsip minimalisasi data.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CT.DM-P8	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan dan menggabungkan prinsip minimalisasi data.	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomen dasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaa n enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.
CT.DM-P8	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan dan menggabungkan prinsip minimalisasi data.	redshift-audit-logging-enabled	Untuk menangkap informasi tentang koneksi dan aktivitas pengguna di klaster Amazon Redshift, pastikan pencatatan audit diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CT.DM-P8	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan dan menggabungkan prinsip minimalisasi data.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CT.DM-P8	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan dan menggabungkan prinsip minimalisasi data.	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CT.DM-P8	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan dan menggabungkan prinsip minimalisasi data.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CT.DM-P8	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan dan menggabungkan prinsip minimalisasi data.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CT.DM-P8	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan dan menggabungkan prinsip minimalisasi data.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CT.DM-P8	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan dan menggabungkan prinsip minimalisasi data.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CT.DM-P8	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan dan menggabungkan prinsip minimalisasi data.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.
CT.DM-P8	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan dan menggabungkan prinsip minimalisasi data.	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CT.DM-P8	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan dan menggabungkan prinsip minimalisasi data.	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
CT.DM-P8	Catatan audit/ log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan dan menggabungkan prinsip minimalisasi data.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
ID.DE-P2	Pihak ekosistem pemrosesan data (misalnya, penyedia layanan, pelanggan, mitra, produsen produk, pengembang aplikasi) diidentifikasi, diprioritaskan, dan dinilai menggunakan proses penilaian risiko privasi.	annual-risk-assessment-performed(Pemeriksaan Proses)	Lakukan penilaian risiko tahunan pada organisasi Anda. Penilaian risiko dapat membantu dalam menentukan kemungkinan dan dampak dari risiko dan/atau kerentanan yang diidentifikasi yang mempengaruhi suatu organisasi.
PR.AC-P1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk individu, proses, dan perangkat yang berwenang.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk individu, proses, dan perangkat yang berwenang.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk individu, proses, dan perangkat yang berwenang.	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk individu, proses, dan perangkat yang berwenang.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk individu, proses, dan perangkat yang berwenang.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk individu, proses, dan perangkat yang berwenang.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsageUsia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk individu, proses, dan perangkat yang berwenang.	secretsmanager-rotation-enabled-check	Aturan ini memastikan AWS rahasia Secrets Manager telah diaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk individu, proses, dan perangkat yang berwenang.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk individu, proses, dan perangkat yang berwenang.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.
PR.AC-P1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk individu, proses, dan perangkat yang berwenang.	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk individu, proses, dan perangkat yang berwenang.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
PR.AC-P1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk individu, proses, dan perangkat yang berwenang.	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk individu, proses, dan perangkat yang berwenang.	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk individu, proses, dan perangkat yang berwenang.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk individu, proses, dan perangkat yang berwenang.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.
PR.AC-P1	Identitas dan kredensil dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk individu, proses, dan perangkat yang berwenang.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P3	Akses jarak jauh dikelola.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.AC-P3	Akses jarak jauh dikelola.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.AC-P3	Akses jarak jauh dikelola.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P3	Akses jarak jauh dikelola.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P3	Akses jarak jauh dikelola.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P3	Akses jarak jauh dikelola.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P3	Akses jarak jauh dikelola.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P3	Akses jarak jauh dikelola.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P3	Akses jarak jauh dikelola.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P3	Akses jarak jauh dikelola.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
PR.AC-P3	Akses jarak jauh dikelola.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P3	Akses jarak jauh dikelola.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.AC-P3	Akses jarak jauh dikelola.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P3	Akses jarak jauh dikelola.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P3	Akses jarak jauh dikelola.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P3	Akses jarak jauh dikelola.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P3	Akses jarak jauh dikelola.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
PR.AC-P3	Akses jarak jauh dikelola.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P3	Akses jarak jauh dikelola.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
PR.AC-P3	Akses jarak jauh dikelola.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P3	Akses jarak jauh dikelola.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P3	Akses jarak jauh dikelola.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P3	Akses jarak jauh dikelola.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P3	Akses jarak jauh dikelola.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P3	Akses jarak jauh dikelola.	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositor i data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsageUsia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P4	Izin akses dan otorisasi dikelola, menggabungkan prinsip-prinsip hak istimewa paling sedikit dan pemisahan tugas.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
PR.AC-P5	Integritas jaringan dilindungi (misalnya, segregasi jaringan, segmentasi jaringan).	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan).	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.AC-P5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan).	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan).	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan).	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .
PR.AC-P5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan).	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan).	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSear ch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerluka n gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan).	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan).	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan).	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.AC-P5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan).	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan).	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan).	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan).	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.AC-P5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan).	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan).	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan).	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan).	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan).	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
PR.AC-P5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan).	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan).	sagemaker-notebook -no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
PR.AC-P5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan).	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan).	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/ 0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan).	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
PR.AC-P5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan).	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P5	Integritas jaringan dilindungi (misalnya , segregasi jaringan, segmentasi jaringan).	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositor i data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P6	Individu dan perangkat dibuktikan dan terikat pada kredensi, dan diautentikasi sepadan dengan risiko transaksi (misalnya, risiko keamanan dan privasi individu dan risiko organisasi lainnya).	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P6	Individu dan perangkat dibuktikan dan terikat pada kredensi, dan diautentikasi sepadan dengan risiko transaksi (misalnya, risiko keamanan dan privasi individu dan risiko organisasi lainnya).	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P6	Individu dan perangkat dibuktikan dan terikat pada kredensi, dan diautentikasi sepadan dengan risiko transaksi (misalnya, risiko keamanan dan privasi individu dan risiko organisasi lainnya).	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P6	Individu dan perangkat dibuktikan dan terikat pada kredensi, dan diautentikasi sepadan dengan risiko transaksi (misalnya, risiko keamanan dan privasi individu dan risiko organisasi lainnya).	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.AC-P6	Individu dan perangkat dibuktikan dan terikat pada kredensi, dan diautentikasi sepadan dengan risiko transaksi (misalnya, risiko keamanan dan privasi individu dan risiko organisasi lainnya).	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
PR.DS-P1	Data-at-rest dilindungi.	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P1	Data-at-rest dilindungi.	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.
PR.DS-P1	Data-at-rest dilindungi.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P1	Data-at-rest dilindungi.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
PR.DS-P1	Data-at-rest dilindungi.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
PR.DS-P1	Data-at-rest dilindungi.	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P1	Data-at-rest dilindungi.	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
PR.DS-P1	Data-at-rest dilindungi.	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P1	Data-at-rest dilindungi.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
PR.DS-P1	Data-at-rest dilindungi.	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P1	Data-at-rest dilindungi.	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P1	Data-at-rest dilindungi.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P1	Data-at-rest dilindungi.	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
PR.DS-P1	Data-at-rest dilindungi.	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P1	Data-at-rest dilindungi.	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
PR.DS-P1	Data-at-rest dilindungi.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P1	Data-at-rest dilindungi.	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P1	Data-at-rest dilindungi.	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P1	Data-at-rest dilindungi.	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
PR.DS-P2	Data-in-transit dilindungi.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P2	Data-in-transit dilindungi.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
PR.DS-P2	Data-in-transit dilindungi.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P2	Data-in-transit dilindungi.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
PR.DS-P2	Data-in-transit dilindungi.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga.	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga.	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga.	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga.	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P4	Kapasitas yang memadai untuk memastikan ketersedi aan tetap terjaga.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga.	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga.	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P4	Kapasitas yang memadai untuk memastikan ketersedi aan tetap terjaga.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P4	Kapasitas yang memadai untuk memastikan ketersedi aan tetap terjaga.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P4	Kapasitas yang memadai untuk memastikan ketersedi aan tetap terjaga.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga.	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga.	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
PR.DS-P4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga.	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga.	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P4	Kapasitas yang memadai untuk memastikan ketersediaan tetap terjaga.	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
PR.DS-P5	Perlindungan terhadap kebocoran data diterapkan.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P5	Perlindungan terhadap kebocoran data diterapkan.	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomen dasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaa n enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P5	Perlindungan terhadap kebocoran data diterapkan.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P5	Perlindungan terhadap kebocoran data diterapkan.	codebuild-project-envvar-awscred-periksa	Pastikan kredensi otentikasi AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild. Jangan menyimpan variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.
PR.DS-P5	Perlindungan terhadap kebocoran data diterapkan.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P5	Perlindungan terhadap kebocoran data diterapkan.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.DS-P5	Perlindungan terhadap kebocoran data diterapkan.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P5	Perlindungan terhadap kebocoran data diterapkan.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P5	Perlindungan terhadap kebocoran data diterapkan.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P5	Perlindungan terhadap kebocoran data diterapkan.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
PR.DS-P5	Perlindungan terhadap kebocoran data diterapkan.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P5	Perlindungan terhadap kebocoran data diterapkan.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.DS-P5	Perlindungan terhadap kebocoran data diterapkan.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P5	Perlindungan terhadap kebocoran data diterapkan.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P5	Perlindungan terhadap kebocoran data diterapkan.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P5	Perlindungan terhadap kebocoran data diterapkan.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P5	Perlindungan terhadap kebocoran data diterapkan.	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P5	Perlindungan terhadap kebocoran data diterapkan.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
PR.DS-P5	Perlindungan terhadap kebocoran data diterapkan.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P5	Perlindungan terhadap kebocoran data diterapkan.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
PR.DS-P5	Perlindungan terhadap kebocoran data diterapkan.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.DS-P5	Perlindungan terhadap kebocoran data diterapkan.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
PR.DS-P6	Mekanisme pemeriksaan integritas digunakan untuk memverifikasi perangkat lunak, firmware, dan integritas informasi.	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.MA-P2	Pemeliharaan aset organisasi dari jarak jauh disetujui, dicatat, dan dilakukan dengan cara yang mencegah akses yang tidak sah.	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomen dasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaa n enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.MA-P2	Pemeliharaan aset organisasi dari jarak jauh disetujui, dicatat, dan dilakukan dengan cara yang mencegah akses yang tidak sah.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P1	Konfigurasi dasar teknologi informasi dibuat dan dipelihara dengan menggabungkan prinsip-prinsip keamanan (misalnya, konsep fungsionalitas terkecil).	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P1	Konfigurasi dasar teknologi informasi dibuat dan dipelihara dengan menggabun gkan prinsip-prinsip keamanan (misalnya, konsep fungsionalitas terkecil).	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P1	Konfigurasi dasar teknologi informasi dibuat dan dipelihara dengan menggabungkan prinsip-prinsip keamanan (misalnya, konsep fungsionalitas terkecil).	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P1	Konfigurasi dasar teknologi informasi dibuat dan dipelihara dengan menggabungkan prinsip-prinsip keamanan (misalnya, konsep fungsionalitas terkecil).	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.
PR.PO-P1	Konfigurasi dasar teknologi informasi dibuat dan dipelihara dengan menggabungkan prinsip-prinsip keamanan (misalnya, konsep fungsionalitas terkecil).	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P1	Konfigurasi dasar teknologi informasi dibuat dan dipelihara dengan menggabungkan prinsip-prinsip keamanan (misalnya, konsep fungsionalitas terkecil).	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P1	Konfigurasi dasar teknologi informasi dibuat dan dipelihara dengan menggabungkan prinsip-prinsip keamanan (misalnya, konsep fungsionalitas terkecil).	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P1	Konfigurasi dasar teknologi informasi dibuat dan dipelihara dengan menggabungkan prinsip-prinsip keamanan (misalnya, konsep fungsionalitas terkecil).	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastikan bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.
AT-1: PR.PO-P10	Rencana manajemen kerentanan dikembangkan dan diimplementasikan.	vuln-management-plan-exists(Pemeriksaan Proses)	Pastikan rencana manajemen kerentanan dikembangkan dan diimplementasikan untuk memiliki proses yang ditentukan secara formal untuk mengatasi kerentanan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P2	Proses kontrol perubahan konfigurasi ditetapkan dan di tempat.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P2	Proses kontrol perubahan konfigurasi ditetapkan dan di tempat.	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P3	Pencadangan informasi dilakukan, dipelihara, dan diuji.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P3	Pencadangan informasi dilakukan, dipelihara, dan diuji.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P3	Pencadangan informasi dilakukan, dipelihara, dan diuji.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P3	Pencadangan informasi dilakukan, dipelihara, dan diuji.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P3	Pencadangan informasi dilakukan, dipelihara, dan diuji.	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P3	Pencadangan informasi dilakukan, dipelihara, dan diuji.	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P3	Pencadangan informasi dilakukan, dipelihara, dan diuji.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P3	Pencadangan informasi dilakukan, dipelihara, dan diuji.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P3	Pencadangan informasi dilakukan, dipelihara, dan diuji.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P3	Pencadangan informasi dilakukan, dipelihara, dan diuji.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P3	Pencadangan informasi dilakukan, dipelihara, dan diuji.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P3	Pencadangan informasi dilakukan, dipelihara, dan diuji.	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P3	Pencadangan informasi dilakukan, dipelihara, dan diuji.	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P3	Pencadangan informasi dilakukan, dipelihara, dan diuji.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P3	Pencadangan informasi dilakukan, dipelihara, dan diuji.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
PR.PO-P3	Pencadangan informasi dilakukan, dipelihara, dan diuji.	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P3	Pencadangan informasi dilakukan, dipelihara, dan diuji.	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P3	Pencadangan informasi dilakukan, dipelihara, dan diuji.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P3	Pencadangan informasi dilakukan, dipelihara, dan diuji.	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P7	Rencana respons (Respon Insiden dan Kesinambu ngan Bisnis) dan rencana pemulihan (Pemulihan Insiden dan Pemulihan Bencana) ditetapka n, di tempat, dan dikelola.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P7	Rencana respons (Respon Insiden dan Kesinambu ngan Bisnis) dan rencana pemulihan (Pemulihan Insiden dan Pemulihan Bencana) ditetapka n, di tempat, dan dikelola.	dynamodb-in-backup-plan	Untuk membantu proses pencadang an data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P7	Rencana respons (Respon Insiden dan Kesinambungan Bisnis) dan rencana pemulihan (Pemulihan Insiden dan Pemulihan Bencana) ditetapkan, di tempat, dan dikelola.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P7	Rencana respons (Respon Insiden dan Kesinambu ngan Bisnis) dan rencana pemulihan (Pemulihan Insiden dan Pemulihan Bencana) ditetapka n, di tempat, dan dikelola.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P7	Rencana respons (Respon Insiden dan Kesinambu ngan Bisnis) dan rencana pemulihan (Pemulihan Insiden dan Pemulihan Bencana) ditetapka n, di tempat, dan dikelola.	efs-in-backup-plan	Untuk membantu proses pencadang an data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P7	Rencana respons (Respon Insiden dan Kesinambu ngan Bisnis) dan rencana pemulihan (Pemulihan Insiden dan Pemulihan Bencana) ditetapka n, di tempat, dan dikelola.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P7	Rencana respons (Respon Insiden dan Kesinambu ngan Bisnis) dan rencana pemulihan (Pemulihan Insiden dan Pemulihan Bencana) ditetapka n, di tempat, dan dikelola.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P7	Rencana respons (Respon Insiden dan Kesinambungan Bisnis) dan rencana pemulihan (Pemulihan Insiden dan Pemulihan Bencana) ditetapkan, di tempat, dan dikelola.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P7	Rencana respons (Respon Insiden dan Kesinambu ngan Bisnis) dan rencana pemulihan (Pemulihan Insiden dan Pemulihan Bencana) ditetapka n, di tempat, dan dikelola.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P7	Rencana respons (Respon Insiden dan Kesinambu ngan Bisnis) dan rencana pemulihan (Pemulihan Insiden dan Pemulihan Bencana) ditetapka n, di tempat, dan dikelola.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P7	Rencana respons (Respon Insiden dan Kesinambungan Bisnis) dan rencana pemulihan (Pemulihan Insiden dan Pemulihan Bencana) ditetapkan, di tempat, dan dikelola.	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P7	Rencana respons (Respon Insiden dan Kesinambungan Bisnis) dan rencana pemulihan (Pemulihan Insiden dan Pemulihan Bencana) ditetapkan, di tempat, dan dikelola.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P7	Rencana respons (Respon Insiden dan Kesinambu ngan Bisnis) dan rencana pemulihan (Pemulihan Insiden dan Pemulihan Bencana) ditetapka n, di tempat, dan dikelola.	backup-recovery-po int-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
PR.PO-P7	Rencana respons (Respon Insiden dan Kesinambu ngan Bisnis) dan rencana pemulihan (Pemulihan Insiden dan Pemulihan Bencana) ditetapka n, di tempat, dan dikelola.	backup-recovery-po int-manual-penghap usan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapus an titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapus an titik pemulihan dapat membantu mencegah penghapus an yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P7	Rencana respons (Respon Insiden dan Kesinambungan Bisnis) dan rencana pemulihan (Pemulihan Insiden dan Pemulihan Bencana) ditetapkan, di tempat, dan dikelola.	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P7	Rencana respons (Respon Insiden dan Kesinambungan Bisnis) dan rencana pemulihan (Pemulihan Insiden dan Pemulihan Bencana) ditetapkan, di tempat, dan dikelola.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PO-P7	Rencana respons (Respon Insiden dan Kesinambu ngan Bisnis) dan rencana pemulihan (Pemulihan Insiden dan Pemulihan Bencana) ditetapka n, di tempat, dan dikelola.	fsx-resources-prot ected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.
PR.PO-P8	Rencana respons dan pemulihan diuji.	response-plan-test ed(Pemeriksaan Proses)	Pastikan respon Insiden dan rencana pemulihan diuji. Ini dapat membantu dalam memahami apakah rencana Anda akan efektif selama insiden dan jika ada celah atau pembaruan yang perlu ditangani.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P2	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.PT-P2	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P2	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting.	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P2	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.
PR.PT-P2	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotens i menyebabkan degradasi ketersedi aan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P2	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSear ch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerluka n gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P3	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P2	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.PT-P2	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P2	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfigurasi sistem untuk hanya menyediakan kemampuan penting.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P2	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
PR.PT-P2	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P2	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.PT-P2	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P2	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P2	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P2	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
PR.PT-P2	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P2	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurk an ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
PR.PT-P2	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting.	s3- bucket-policy-gran tee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_ bucket_policy_gran tee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P2	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting.	ec2- instance-profile-a ttached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirk an profil instans ke instans Anda dapat membantu pengelola an hak istimewa dan izin paling sedikit.
PR.PT-P2	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting.	ssm-document-not-p ublic	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkin kan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspo s informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P2	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfig urasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P2	Prinsip fungsionalitas terkecil digabungkan dengan mengkonfi gurasi sistem untuk hanya menyediakan kemampuan penting.	redshift-enhanced-vpc-routing-diaktifkan	Perutean VPC yang disempurnakan memaksa semua lalu lintas COPY dan UNLOAD antara cluster dan repositor i data untuk melewati VPC Amazon Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan log aliran VPC untuk memantau lalu lintas jaringan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P3	Jaringan komunikasi dan kontrol dilindungi.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P3	Jaringan komunikasi dan kontrol dilindungi.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P3	Jaringan komunikasi dan kontrol dilindungi.	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
PR.PT-P3	Jaringan komunikasi dan kontrol dilindungi.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P3	Jaringan komunikasi dan kontrol dilindungi.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.PT-P3	Jaringan komunikasi dan kontrol dilindungi.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P3	Jaringan komunikasi dan kontrol dilindungi.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.PT-P3	Jaringan komunikasi dan kontrol dilindungi.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSear ch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerluka n gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P3	Jaringan komunikasi dan kontrol dilindungi.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P3	Jaringan komunikasi dan kontrol dilindungi.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.PT-P3	Jaringan komunikasi dan kontrol dilindungi.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P3	Jaringan komunikasi dan kontrol dilindungi.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P3	Jaringan komunikasi dan kontrol dilindungi.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
PR.PT-P3	Jaringan komunikasi dan kontrol dilindungi.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P3	Jaringan komunikasi dan kontrol dilindungi.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P3	Jaringan komunikasi dan kontrol dilindungi.	s3- account-level-publ ic-access -blok-per iodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P3	Jaringan komunikasi dan kontrol dilindungi.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
PR.PT-P3	Jaringan komunikasi dan kontrol dilindungi.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P3	Jaringan komunikasi dan kontrol dilindungi.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P3	Jaringan komunikasi dan kontrol dilindungi.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P3	Jaringan komunikasi dan kontrol dilindungi.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P3	Jaringan komunikasi dan kontrol dilindungi.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.
PR.PT-P3	Jaringan komunikasi dan kontrol dilindungi.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P3	Jaringan komunikasi dan kontrol dilindungi.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
PR.PT-P3	Jaringan komunikasi dan kontrol dilindungi.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P4	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan.	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemelihar aan kapasitas dan ketersediaan yang memadai. Penyeimba ng beban secara berkala mengirimk an ping, mencoba koneksi, atau mengirim permintaa n untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika sebuah instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P4	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan.	dynamodb-in-backup-plan	Untuk membantu proses pencadang an data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P4	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P4	Mekanisme (misalnya, failsafe, load balancing, hot swap) diterapkan untuk mencapai persyaratan ketahanan dalam situasi normal dan merugikan.	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P4	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan.	dynamodb-pitr-enab led	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertah ankan cadangan dengan memastika n bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P4	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P4	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan.	elb-cross-zone-loa d-menyeimbangkan diaktifkan	Aktifkan penyeimba ngan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimba ngan beban lintas zona mengurang i kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkat kan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P4	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan.	efs-in-backup-plan	Untuk membantu proses pencadang an data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P4	Mekanisme (misalnya, failsafe, load balancing, hot swap) diterapkan untuk mencapai persyaratan ketahanan dalam situasi normal dan merugikan.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P4	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P4	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P4	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersedi aan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplika si data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastru ktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutk an operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P4	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan.	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relationa l Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindun gan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersedi aan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P4	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P4	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan.	redshift-backup-en abled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifka n untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P4	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P4	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan.	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimpleme ntasikan untuk mencapai persyarat an ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivi tas jika salah satu koneksi Site-to-S ite VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivi tas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P4	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan.	aurora-resources-p rotected-by-rencana cadangan	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P4	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan.	backup-plan-min-fr equency-and-min-re tention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkin kan Anda untuk mengatur parameter requiredFrequencyV alue (Config default: 1), (requiredR etentionDays Config default: 35) dan (requiredFrequencyU nit Config default: days). Nilai aktual harus mencerminkan persyaratan organisas i Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P4	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
PR.PT-P4	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan.	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapus an titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapus an titik pemulihan dapat membantu mencegah penghapus an yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P4	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan.	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadang an data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkin kan Anda untuk mengatur parameter requiredRetentionD ays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisas i Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P4	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadang an data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
PR.PT-P4	Mekanisme (misalnya , failsafe, load balancing, hot swap) diterapkan untuk mencapai persyarat an ketahanan dalam situasi normal dan merugikan.	fsx-resources-prot ected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Kerangka Privasi NIST v1.0.

Praktik Terbaik Operasional untuk NYDFS 23

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara persyaratan keamanan siber Departemen Layanan Keuangan Negara Bagian New York (NYDFS) untuk perusahaan jasa keuangan (23 NYCRR 500) dan aturan Config yang dikelola. AWS Setiap AWS Config aturan berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau lebih kontrol NYDFS AS. Kontrol NYDFS 23 NYCRR 500 AS dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasiaan, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasiaan, integritas, dan ketersediaan Sistem	alb-http-to-https-pemeriksaan-pengalihan	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Informasi Entitas yang Tercakup.		data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasia an, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	api-gw-cache-enabl ed-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasia an, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrai l jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasia an, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasia an, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasiaan, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasiaan, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasia an, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasia an, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasiaan, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasia an, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasia an, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasia an, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	s3- bucket-ssl-request s-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasia an, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	sagemaker-endpoint -configuration-kms- kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasia an, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasia an, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasia an, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasia an, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	rds-snapshot-encry pted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasia an, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	alb-http-drop-invalid-Header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasiaan, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	kinesis-stream-encrypted	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasiaan, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasia an, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasiaan, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasiaan, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasiaan, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasiaan, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instance siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasiaan, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasiaan, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasiaan, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasia an, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relationa l Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindun gan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersedi aan untuk aplikasi Anda.
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasia an, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasiaan, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasia an, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	autoscaling-launch -config-public-ip- dinonaktifkan	Jika Anda mengonfig urasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasia an, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	backup-recovery-po int-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasiaan, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasiaan, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasiaan, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasia an, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasiaan, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasia an, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	s3- default-encryption -kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasia an, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	ssm-document-not-p ublic	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkin kan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspo s informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasia an, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	opensearch-encrypt ed-at-rest	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk domain OpenSearc h Layanan Amazon Anda.
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasia an, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	opensearch-node-to -node-pemeriksaan enkripsi-	Pastikan node-to-n ode enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkrip si memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.02 (a)	(a) Program Keamanan Siber. Setiap Entitas yang Tercakup harus memelihara program keamanan siber yang dirancang untuk melindungi kerahasiaan, integritas, dan ketersediaan Sistem Informasi Entitas yang Tercakup.	codebuild-project-artifact-encryption	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk AWS CodeBuild artefak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredenal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	dibatasi ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/ 0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindunginya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (2)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (2) menggunakan infrastruktur defensif dan penerapan kebijakan dan prosedur untuk melindungi Sistem Informasi Entitas yang Tercakup, dan Informasi Nonpublik yang disimpan pada Sistem Informasi tersebut, dari akses, penggunaan, atau tindakan jahat lainnya yang tidak sah.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (3)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (3) mendeteksi Peristiwa Keamanan Siber.	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (3)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (3) mendeteksi Peristiwa Keamanan Siber.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (3)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (3) mendeteksi Peristiwa Keamanan Siber.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (3)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (3) mendeteksi Peristiwa Keamanan Siber.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
500,02 (b) (3)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (3) mendeteksi Peristiwa Keamanan Siber.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (3)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (3) mendeteksi Peristiwa Keamanan Siber.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
500,02 (b) (3)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (3) mendeteksi Peristiwa Keamanan Siber.	redshift-audit-logging-enabled	Untuk menangkap informasi tentang koneksi dan aktivitas pengguna di klaster Amazon Redshift, pastikan pencatatan audit diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (3)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (3) mendeteksi Peristiwa Keamanan Siber.	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.
500,02 (b) (3)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (3) mendeteksi Peristiwa Keamanan Siber.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (3)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (3) mendeteksi Peristiwa Keamanan Siber.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (3)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (3) mendeteksi Peristiwa Keamanan Siber.	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (3)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (3) mendeteksi Peristiwa Keamanan Siber.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
500,02 (b) (3)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (3) mendeteksi Peristiwa Keamanan Siber.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (3)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (3) mendeteksi Peristiwa Keamanan Siber.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (3)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (3) mendeteksi Peristiwa Keamanan Siber.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (3)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (3) mendeteksi Peristiwa Keamanan Siber.	opensearch-audit-logging-enabled	Pastikan pencatatan audit diaktifkan di domain OpenSearch Layanan Amazon Anda. Pencatatan audit memungkinkan Anda melacak aktivitas pengguna di OpenSearch domain Anda, termasuk keberhasilan dan kegagalan otentikasi, permintaan, perubahan indeks OpenSearch, dan kueri penelusuran yang masuk.
500,02 (b) (3)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (3) mendeteksi Peristiwa Keamanan Siber.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (3)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (3) mendeteksi Peristiwa Keamanan Siber.	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi terperinci tentang proyek build Anda.
500,02 (b) (3)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (3) mendeteksi Peristiwa Keamanan Siber.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (3)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (3) mendeteksi Peristiwa Keamanan Siber.	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (3)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (3) mendeteksi Peristiwa Keamanan Siber.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (5)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (5) pemulihan dari Kejadian Keamanan Siber dan memulihkan operasi dan layanan normal.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (5)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (5) pemulihan dari Kejadian Keamanan Siber dan memulihkan operasi dan layanan normal.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (5)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (5) pemulihan dari Kejadian Keamanan Siber dan memulihkan operasi dan layanan normal.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan cadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (5)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (5) pemulihan dari Kejadian Keamanan Siber dan memulihkan operasi dan layanan normal.	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan tambahan, kapasitas khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (5)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (5) pemulihan dari Kejadian Keamanan Siber dan memulihka n operasi dan layanan normal.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (5)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (5) pemulihan dari Kejadian Keamanan Siber dan memulihka n operasi dan layanan normal.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (5)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (5) pemulihan dari Kejadian Keamanan Siber dan memulihka n operasi dan layanan normal.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (5)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (5) pemulihan dari Kejadian Keamanan Siber dan memulihkan operasi dan layanan normal.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (5)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (5) pemulihan dari Kejadian Keamanan Siber dan memulihkan operasi dan layanan normal.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (5)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (5) pemulihan dari Kejadian Keamanan Siber dan memulihkan operasi dan layanan normal.	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (5)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (5) pemulihan dari Kejadian Keamanan Siber dan memulihkan operasi dan layanan normal.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relational Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (5)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (5) pemulihan dari Kejadian Keamanan Siber dan memulihkan operasi dan layanan normal.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,02 (b) (5)	(b) Program keamanan siber harus didasarkan pada Penilaian Risiko Entitas yang Tercakup dan dirancang untuk menjalankan fungsi keamanan siber inti berikut: (5) pemulihan dari Kejadian Keamanan Siber dan memulihkan operasi dan layanan normal.	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,05	Program keamanan siber untuk setiap entitas yang tercakup harus mencakup pemantauan dan pengujian, yang dikembangkan sesuai dengan penilaian risiko entitas yang tercakup, yang dirancang untuk menilai efektivitas program keamanan siber entitas yang tercakup. Pemantaua n dan pengujian harus mencakup pemantaua n berkelanjutan atau pengujian penetrasi berkala dan penilaian kerentanan. Tidak adanya pemantaua n berkelanjutan yang efektif, atau sistem lain untuk mendeteksi, secara berkelanjutan, perubahan dalam sistem informasi yang dapat menciptak an atau menunjukk an kerentanan, entitas yang tercakup harus melakukan : (a) pengujian	vuln-management-pl an-exists (pemeriks aan proses)	Pastikan rencana manajemen kerentana n dikembangkan dan diimplementasikan untuk memiliki proses yang ditentukan secara formal untuk mengatasi kerentanan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	penetrasi tahunan terhadap sistem informasi entitas yang tercakup yang ditentukan setiap tahun berdasarkan risiko yang diidentif ikasi yang relevan sesuai dengan penilaian risiko; dan (b) penilaian kerentanan dua tahunan, termasuk pemindaian sistemati s atau tinjauan sistem informasi yang dirancang secara wajar untuk mengidentifikasi kerentanan keamanan siber yang diketahui publik kemampuan dalam mencakup sistem informasi entitas berdasarkan penilaian risiko.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.06 (a)	(a) Setiap Entitas yang Tercakup harus secara aman memelihara sistem yang, sejauh berlaku dan berdasarkan Penilaian Risikonya : (1) dirancang untuk merekonstruksi transaksi keuangan material yang cukup untuk mendukung operasi dan kewajiban normal Entitas yang Tercakup; dan (2) mencakup jejak audit yang dirancang untuk mendeteks i dan menanggapi Peristiwa Keamanan Siber yang memiliki kemungkinan wajar untuk secara material merugikan bagian material apa pun dari operasi normal Entitas yang Tercakup.	api-gw-execution-l ogging-diaktifkan	Pencatatan API Gateway menampilk an tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.06 (a)	(a) Setiap Entitas yang Tercakup harus secara aman memelihara sistem yang, sejauh berlaku dan berdasarkan Penilaian Risikonya : (1) dirancang untuk merekonstruksi transaksi keuangan material yang cukup untuk mendukung operasi dan kewajiban normal Entitas yang Tercakup; dan (2) mencakup jejak audit yang dirancang untuk mendeteks i dan menanggapi Peristiwa Keamanan Siber yang memiliki kemungkinan wajar untuk secara material merugikan bagian material apa pun dari operasi normal Entitas yang Tercakup.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.06 (a)	(a) Setiap Entitas yang Tercakup harus secara aman memelihara sistem yang, sejauh berlaku dan berdasarkan Penilaian Risikonya : (1) dirancang untuk merekonstruksi transaksi keuangan material yang cukup untuk mendukung operasi dan kewajiban normal Entitas yang Tercakup; dan (2) mencakup jejak audit yang dirancang untuk mendeteks i dan menanggapi Peristiwa Keamanan Siber yang memiliki kemungkinan wajar untuk secara material merugikan bagian material apa pun dari operasi normal Entitas yang Tercakup.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.06 (a)	(a) Setiap Entitas yang Tercakup harus secara aman memelihara sistem yang, sejauh berlaku dan berdasarkan Penilaian Risikonya : (1) dirancang untuk merekonstruksi transaksi keuangan material yang cukup untuk mendukung operasi dan kewajiban normal Entitas yang Tercakup; dan (2) mencakup jejak audit yang dirancang untuk mendeteks i dan menanggapi Peristiwa Keamanan Siber yang memiliki kemungkinan wajar untuk secara material merugikan bagian material apa pun dari operasi normal Entitas yang Tercakup.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteks i aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.06 (a)	(a) Setiap Entitas yang Tercakup harus secara aman memelihara sistem yang, sejauh berlaku dan berdasarkan Penilaian Risikonya : (1) dirancang untuk merekonstruksi transaksi keuangan material yang cukup untuk mendukung operasi dan kewajiban normal Entitas yang Tercakup; dan (2) mencakup jejak audit yang dirancang untuk mendeteks i dan menanggapi Peristiwa Keamanan Siber yang memiliki kemungkinan wajar untuk secara material merugikan bagian material apa pun dari operasi normal Entitas yang Tercakup.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.06 (a)	(a) Setiap Entitas yang Tercakup harus secara aman memelihara sistem yang, sejauh berlaku dan berdasarkan Penilaian Risikonya : (1) dirancang untuk merekonstruksi transaksi keuangan material yang cukup untuk mendukung operasi dan kewajiban normal Entitas yang Tercakup; dan (2) mencakup jejak audit yang dirancang untuk mendeteks i dan menanggapi Peristiwa Keamanan Siber yang memiliki kemungkinan wajar untuk secara material merugikan bagian material apa pun dari operasi normal Entitas yang Tercakup.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.06 (a)	(a) Setiap Entitas yang Tercakup harus secara aman memelihara sistem yang, sejauh berlaku dan berdasarkan Penilaian Risikonya : (1) dirancang untuk merekonstruksi transaksi keuangan material yang cukup untuk mendukung operasi dan kewajiban normal Entitas yang Tercakup; dan (2) mencakup jejak audit yang dirancang untuk mendeteks i dan menanggapi Peristiwa Keamanan Siber yang memiliki kemungkinan wajar untuk secara material merugikan bagian material apa pun dari operasi normal Entitas yang Tercakup.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediak an metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinc i untuk permintaa n yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.06 (a)	(a) Setiap Entitas yang Tercakup harus secara aman memelihara sistem yang, sejauh berlaku dan berdasarkan Penilaian Risikonya : (1) dirancang untuk merekonstruksi transaksi keuangan material yang cukup untuk mendukung operasi dan kewajiban normal Entitas yang Tercakup; dan (2) mencakup jejak audit yang dirancang untuk mendeteks i dan menanggapi Peristiwa Keamanan Siber yang memiliki kemungkinan wajar untuk secara material merugikan bagian material apa pun dari operasi normal Entitas yang Tercakup.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.06 (a)	(a) Setiap Entitas yang Tercakup harus secara aman memelihara sistem yang, sejauh berlaku dan berdasarkan Penilaian Risikonya : (1) dirancang untuk merekonstruksi transaksi keuangan material yang cukup untuk mendukung operasi dan kewajiban normal Entitas yang Tercakup; dan (2) mencakup jejak audit yang dirancang untuk mendeteks i dan menanggapi Peristiwa Keamanan Siber yang memiliki kemungkinan wajar untuk secara material merugikan bagian material apa pun dari operasi normal Entitas yang Tercakup.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.06 (a)	(a) Setiap Entitas yang Tercakup harus secara aman memelihara sistem yang, sejauh berlaku dan berdasarkan Penilaian Risikonya : (1) dirancang untuk merekonstruksi transaksi keuangan material yang cukup untuk mendukung operasi dan kewajiban normal Entitas yang Tercakup; dan (2) mencakup jejak audit yang dirancang untuk mendeteks i dan menanggapi Peristiwa Keamanan Siber yang memiliki kemungkinan wajar untuk secara material merugikan bagian material apa pun dari operasi normal Entitas yang Tercakup.	codebuild-project-logging-enabled	Pastikan pencatata n AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatc h atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi terperinci tentang proyek build Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.06 (a)	(a) Setiap Entitas yang Tercakup harus secara aman memelihara sistem yang, sejauh berlaku dan berdasarkan Penilaian Risikonya : (1) dirancang untuk merekonstruksi transaksi keuangan material yang cukup untuk mendukung operasi dan kewajiban normal Entitas yang Tercakup; dan (2) mencakup jejak audit yang dirancang untuk mendeteks i dan menanggapi Peristiwa Keamanan Siber yang memiliki kemungkinan wajar untuk secara material merugikan bagian material apa pun dari operasi normal Entitas yang Tercakup.	redshift-audit-logging-enabled	Untuk menangkap informasi tentang koneksi dan aktivitas pengguna di klaster Amazon Redshift, pastikan pencatatan audit diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.06 (a)	(a) Setiap Entitas yang Tercakup harus secara aman memelihara sistem yang, sejauh berlaku dan berdasarkan Penilaian Risikonya : (1) dirancang untuk merekonstruksi transaksi keuangan material yang cukup untuk mendukung operasi dan kewajiban normal Entitas yang Tercakup; dan (2) mencakup jejak audit yang dirancang untuk mendeteks i dan menanggapi Peristiwa Keamanan Siber yang memiliki kemungkinan wajar untuk secara material merugikan bagian material apa pun dari operasi normal Entitas yang Tercakup.	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatata n AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.06 (a)	(a) Setiap Entitas yang Tercakup harus secara aman memelihara sistem yang, sejauh berlaku dan berdasarkan Penilaian Risikonya : (1) dirancang untuk merekonstruksi transaksi keuangan material yang cukup untuk mendukung operasi dan kewajiban normal Entitas yang Tercakup; dan (2) mencakup jejak audit yang dirancang untuk mendeteksi dan menanggapi Peristiwa Keamanan Siber yang memiliki kemungkinan wajar untuk secara material merugikan bagian material apa pun dari operasi normal Entitas yang Tercakup.	opensearch-audit-logging-enabled	Pastikan pencatatan audit diaktifkan di domain OpenSearch Layanan Amazon Anda. Pencatatan audit memungkinkan Anda melacak aktivitas pengguna di OpenSearch domain Anda, termasuk keberhasilan dan kegagalan otentikasi, permintaan, perubahan indeks OpenSearch, dan kueri penelusuran yang masuk.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.06 (a)	(a) Setiap Entitas yang Tercakup harus secara aman memelihara sistem yang, sejauh berlaku dan berdasarkan Penilaian Risikonya : (1) dirancang untuk merekonstruksi transaksi keuangan material yang cukup untuk mendukung operasi dan kewajiban normal Entitas yang Tercakup; dan (2) mencakup jejak audit yang dirancang untuk mendeteksi dan menanggapi Peristiwa Keamanan Siber yang memiliki kemungkinan wajar untuk secara material merugikan bagian material apa pun dari operasi normal Entitas yang Tercakup.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,06 (b)	(b) Setiap Entitas yang Tercakup harus menyimpan catatan yang disyaratkan oleh bagian 500.06 (a) (1) Bagian ini selama tidak kurang dari lima tahun dan harus menyimpan catatan yang disyaratkan oleh bagian 500.06 (a) (2) Bagian ini untuk tidak kurang dari tiga tahun.	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.06 (a)	(a) Setiap Entitas yang Tercakup harus secara aman memelihara sistem yang, sejauh berlaku dan berdasarkan Penilaian Risikonya : (1) dirancang untuk merekonstruksi transaksi keuangan material yang cukup untuk mendukung operasi dan kewajiban normal Entitas yang Tercakup; dan (2) mencakup jejak audit yang dirancang untuk mendeteks i dan menanggapi Peristiwa Keamanan Siber yang memiliki kemungkinan wajar untuk secara material merugikan bagian material apa pun dari operasi normal Entitas yang Tercakup.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.06 (a)	(a) Setiap Entitas yang Tercakup harus secara aman memelihara sistem yang, sejauh berlaku dan berdasarkan Penilaian Risikonya : (1) dirancang untuk merekonstruksi transaksi keuangan material yang cukup untuk mendukung operasi dan kewajiban normal Entitas yang Tercakup; dan (2) mencakup jejak audit yang dirancang untuk mendeteks i dan menanggapi Peristiwa Keamanan Siber yang memiliki kemungkinan wajar untuk secara material merugikan bagian material apa pun dari operasi normal Entitas yang Tercakup.	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	ecs-task-definition-user-for-host-mode-check	Jika definisi tugas memiliki hak istimewa yang tinggi, itu karena pelanggan telah secara khusus ikut serta dalam konfigurasi tersebut. Kontrol ini memeriksa eskalasi hak istimewa yang tidak terduga ketika definisi tugas mengaktifkan jaringan host tetapi pelanggan belum ikut serta dalam hak istimewa yang ditinggikan.
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsageUsia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	secretsmanager-rotation-enabled-check	Aturan ini memastikan AWS rahasia Secrets Manager telah diaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan.
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	secretsmanager-scheduled-rotation-success-periksa	Aturan ini memastikan bahwa AWS rahasia Secrets Manager telah berhasil diputar sesuai dengan jadwal rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode dimana rahasia aktif, dan berpotensi mengurangi dampak bisnis jika dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktifkan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediakan sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.07	Sebagai bagian dari program keamanan sibernya, berdasark an Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigurasi ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.07	Sebagai bagian dari program keamanan sibernya, berdasark an Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
500.07	Sebagai bagian dari program keamanan sibernya, berdasark an Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
500.07	Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko Entitas Tercakup, setiap Entitas yang Tercakup akan membatasi hak akses pengguna ke Sistem Informasi yang menyediakan akses ke Informasi Nonpublik dan secara berkala akan meninjau hak akses tersebut.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,8 (a)	(a) Setiap program keamanan siber Entitas Tercakup harus mencakup prosedur, pedoman, dan standar tertulis yang dirancang untuk memastikan penggunaan praktik pengembangan yang aman untuk aplikasi yang dikembang kan secara internal yang digunakan oleh Entitas Tercakup, dan prosedur untuk mengevaluasi, menilai, atau menguji keamanan aplikasi yang dikembang kan secara eksternal yang digunakan oleh Entitas Tercakup dalam konteks lingkungan teknologi Entitas Tercakup.	codebuild-project-envvar-awscred-periksa	Pastikan kredensya l otentikasi AWS_ACCES S_KEY_ID dan AWS_SECRE T_ACCESS_KEY tidak ada dalam lingkungan proyek AWS Codebuild . Jangan simpan variabel-variabel ini dalam teks yang jelas. Menyimpan variabel-variabel ini dalam teks yang jelas menyebabk an paparan data yang tidak diinginkan dan akses yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500,8 (a)	(a) Setiap program keamanan siber Entitas Tercakup harus mencakup prosedur, pedoman, dan standar tertulis yang dirancang untuk memastikan penggunaan praktik pengembangan yang aman untuk aplikasi yang dikembang kan secara internal yang digunakan oleh Entitas Tercakup, dan prosedur untuk mengevaluasi, menilai, atau menguji keamanan aplikasi yang dikembang kan secara eksternal yang digunakan oleh Entitas Tercakup dalam konteks lingkungan teknologi Entitas Tercakup.	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber Bitbucket GitHub atau Bitbucket tidak berisi token akses pribadi, kredensyal masuk dalam lingkungan proyek Codebuild . AWS Gunakan OAuth alih-alih token akses pribadi atau kredensyal masuk untuk memberika n otorisasi untuk mengakses GitHub atau repositori Bitbucket.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.09	(a) Setiap entitas yang tercakup harus melakukan penilaian risiko berkala terhadap sistem informasi entitas yang tercakup yang cukup untuk menginformasikan desain program keamanan siber sebagaimana disyaratkan oleh Bagian ini. Penilaian risiko tersebut harus diperbarui sebagaimana diperlukan secara wajar untuk mengatasi perubahan pada sistem informasi, informasi nonpublik, atau operasi bisnis entitas yang tercakup. Penilaian risiko entitas yang tercakup akan memungkinkan revisi kontrol untuk menanggapi perkembangan teknologi dan ancaman yang berkembang dan harus mempertimbangkan risiko tertentu dari operasi	annual-risk-assessment-performed (pemeriksaan proses) >	Lakukan penilaian risiko tahunan pada organisasi Anda. Penilaian risiko dapat membantu dalam menentukan kemungkinan dan dampak dari risiko dan/atau kerentanan yang diidentifikasi yang mempengaruhi suatu organisasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	bisnis entitas yang tercakup terkait dengan keamanan siber, informasi nonpublik yang dikumpulkan atau disimpan, sistem informasi yang digunakan dan ketersediaan dan efektivitas kontrol untuk melindungi sistem informasi dan informasi nonpublik.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.12	(a) Otentikasi Multi-Faktor. Berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menggunakan kontrol yang efektif, yang dapat mencakup Otentikasi Multi-Faktor atau Otentikasi Berbasis Risiko, untuk melindungi terhadap akses tidak sah ke Sistem Informasi atau Informasi Nonpublik. (b) Otentikasi Multi-Faktor akan digunakan untuk setiap individu yang mengakses jaringan internal Entitas Tercakup dari jaringan eksternal, kecuali CISO Entitas Tercakup telah menyetujui secara tertulis penggunaan kontrol akses yang setara atau lebih aman secara wajar.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.12	(a) Otentikasi Multi-Faktor. Berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menggunakan kontrol yang efektif, yang dapat mencakup Otentikasi Multi-Faktor atau Otentikasi Berbasis Risiko, untuk melindungi terhadap akses tidak sah ke Sistem Informasi atau Informasi Nonpublik. (b) Otentikasi Multi-Faktor akan digunakan untuk setiap individu yang mengakses jaringan internal Entitas Tercakup dari jaringan eksternal, kecuali CISO Entitas Tercakup telah menyetujui secara tertulis penggunaan kontrol akses yang setara atau lebih aman secara wajar.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.12	(a) Otentikasi Multi-Faktor. Berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menggunakan kontrol yang efektif, yang dapat mencakup Otentikasi Multi-Faktor atau Otentikasi Berbasis Risiko, untuk melindungi terhadap akses tidak sah ke Sistem Informasi atau Informasi Nonpublik. (b) Otentikasi Multi-Faktor akan digunakan untuk setiap individu yang mengakses jaringan internal Entitas Tercakup dari jaringan eksternal, kecuali CISO Entitas Tercakup telah menyetujui secara tertulis penggunaan kontrol akses yang setara atau lebih aman secara wajar.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.12	(a) Otentikasi Multi-Faktor. Berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menggunakan kontrol yang efektif, yang dapat mencakup Otentikasi Multi-Faktor atau Otentikasi Berbasis Risiko, untuk melindungi terhadap akses tidak sah ke Sistem Informasi atau Informasi Nonpublik. (b) Otentikasi Multi-Faktor akan digunakan untuk setiap individu yang mengakses jaringan internal Entitas Tercakup dari jaringan eksternal, kecuali CISO Entitas Tercakup telah menyetujui secara tertulis penggunaan kontrol akses yang setara atau lebih aman secara wajar.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.12	(a) Otentikasi Multi-Faktor. Berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menggunakan kontrol yang efektif, yang dapat mencakup Otentikasi Multi-Faktor atau Otentikasi Berbasis Risiko, untuk melindungi terhadap akses tidak sah ke Sistem Informasi atau Informasi Nonpublik. (b) Otentikasi Multi-Faktor akan digunakan untuk setiap individu yang mengakses jaringan internal Entitas Tercakup dari jaringan eksternal, kecuali CISO Entitas Tercakup telah menyetujui secara tertulis penggunaan kontrol akses yang setara atau lebih aman secara wajar.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.14 (a)	(a) menerapkan kebijakan, prosedur, dan kontrol berbasis risiko yang dirancang untuk memantau aktivitas Pengguna Resmi dan mendeteksi akses atau penggunaan yang tidak sah, atau merusak, Informasi Nonpublik oleh Pengguna Resmi tersebut.	cloudwatch-alarm-action-check	Amazon CloudWatch mempering atkan ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu. Alarm tersebut melakukan satu atau beberapa tindakan berdasarkan pada nilai metrik atau ekspresi relatif terhadap ambang batas selama beberapa periode waktu. Aturan ini memerlukan nilai untuk alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Nilai aktual harus mencerminkan tindakan alarm untuk lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.14 (a)	(a) menerapkan kebijakan, prosedur, dan kontrol berbasis risiko yang dirancang untuk memantau aktivitas Pengguna Resmi dan mendeteksi akses atau penggunaan yang tidak sah, atau merusak, Informasi Nonpublik oleh Pengguna Resmi tersebut.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
500.14 (a)	(a) menerapkan kebijakan, prosedur, dan kontrol berbasis risiko yang dirancang untuk memantau aktivitas Pengguna Resmi dan mendeteksi akses atau penggunaan yang tidak sah, atau merusak, Informasi Nonpublik oleh Pengguna Resmi tersebut.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.14 (a)	(a) menerapkan kebijakan, prosedur, dan kontrol berbasis risiko yang dirancang untuk memantau aktivitas Pengguna Resmi dan mendeteksi akses atau penggunaan yang tidak sah, atau merusak, Informasi Nonpublik oleh Pengguna Resmi tersebut.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
500.14 (a)	(a) menerapkan kebijakan, prosedur, dan kontrol berbasis risiko yang dirancang untuk memantau aktivitas Pengguna Resmi dan mendeteksi akses atau penggunaan yang tidak sah, atau merusak, Informasi Nonpublik oleh Pengguna Resmi tersebut.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.14 (a)	(a) menerapkan kebijakan, prosedur, dan kontrol berbasis risiko yang dirancang untuk memantau aktivitas Pengguna Resmi dan mendeteksi akses atau penggunaan yang tidak sah, atau merusak, Informasi Nonpublik oleh Pengguna Resmi tersebut.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.14 (a)	(a) menerapkan kebijakan, prosedur, dan kontrol berbasis risiko yang dirancang untuk memantau aktivitas Pengguna Resmi dan mendeteksi akses atau penggunaan yang tidak sah, atau merusak, Informasi Nonpublik oleh Pengguna Resmi tersebut.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.14 (a)	(a) menerapkan kebijakan, prosedur, dan kontrol berbasis risiko yang dirancang untuk memantau aktivitas Pengguna Resmi dan mendeteksi akses atau penggunaan yang tidak sah, atau merusak, Informasi Nonpublik oleh Pengguna Resmi tersebut.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.14 (a)	(a) menerapkan kebijakan, prosedur, dan kontrol berbasis risiko yang dirancang untuk memantau aktivitas Pengguna Resmi dan mendeteksi akses atau penggunaan yang tidak sah, atau merusak, Informasi Nonpublik oleh Pengguna Resmi tersebut.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
500.14 (a)	(a) menerapkan kebijakan, prosedur, dan kontrol berbasis risiko yang dirancang untuk memantau aktivitas Pengguna Resmi dan mendeteksi akses atau penggunaan yang tidak sah, atau merusak, Informasi Nonpublik oleh Pengguna Resmi tersebut.	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.14 (a)	(a) menerapkan kebijakan, prosedur, dan kontrol berbasis risiko yang dirancang untuk memantau aktivitas Pengguna Resmi dan mendeteksi akses atau penggunaan yang tidak sah, atau merusak, Informasi Nonpublik oleh Pengguna Resmi tersebut.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
500.14 (a)	(a) menerapkan kebijakan, prosedur, dan kontrol berbasis risiko yang dirancang untuk memantau aktivitas Pengguna Resmi dan mendeteksi akses atau penggunaan yang tidak sah, atau merusak, Informasi Nonpublik oleh Pengguna Resmi tersebut.	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi terperinci tentang proyek build Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.14 (a)	(a) menerapkan kebijakan, prosedur, dan kontrol berbasis risiko yang dirancang untuk memantau aktivitas Pengguna Resmi dan mendeteksi akses atau penggunaan yang tidak sah, atau merusak, Informasi Nonpublik oleh Pengguna Resmi tersebut.	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.14 (a)	(a) menerapkan kebijakan, prosedur, dan kontrol berbasis risiko yang dirancang untuk memantau aktivitas Pengguna Resmi dan mendeteksi akses atau penggunaan yang tidak sah, atau merusak, Informasi Nonpublik oleh Pengguna Resmi tersebut.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.14 (a)	(a) menerapkan kebijakan, prosedur, dan kontrol berbasis risiko yang dirancang untuk memantau aktivitas Pengguna Resmi dan mendeteksi akses atau penggunaan yang tidak sah, atau merusak, Informasi Nonpublik oleh Pengguna Resmi tersebut.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.14 (a)	(a) menerapkan kebijakan, prosedur, dan kontrol berbasis risiko yang dirancang untuk memantau aktivitas Pengguna Resmi dan mendeteksi akses atau penggunaan yang tidak sah, atau merusak, Informasi Nonpublik oleh Pengguna Resmi tersebut.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.14 (a)	(a) menerapkan kebijakan, prosedur, dan kontrol berbasis risiko yang dirancang untuk memantau aktivitas Pengguna Resmi dan mendeteksi akses atau penggunaan yang tidak sah, atau merusak, Informasi Nonpublik oleh Pengguna Resmi tersebut.	opensearch-audit-logging-enabled	Pastikan pencatatan audit diaktifkan di domain OpenSearch Layanan Amazon Anda. Pencatatan audit memungkinkan Anda melacak aktivitas pengguna di OpenSearch domain Anda, termasuk keberhasilan dan kegagalan otentikasi, permintaan, perubahan indeks OpenSearch, dan kueri penelusuran yang masuk.
500.14 (a)	(a) menerapkan kebijakan, prosedur, dan kontrol berbasis risiko yang dirancang untuk memantau aktivitas Pengguna Resmi dan mendeteksi akses atau penggunaan yang tidak sah, atau merusak, Informasi Nonpublik oleh Pengguna Resmi tersebut.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.14 (a)	(a) menerapkan kebijakan, prosedur, dan kontrol berbasis risiko yang dirancang untuk memantau aktivitas Pengguna Resmi dan mendeteksi akses atau penggunaan yang tidak sah, atau merusak, Informasi Nonpublik oleh Pengguna Resmi tersebut.	redshift-audit-logging-enabled	Untuk menangkap informasi tentang koneksi dan aktivitas pengguna di klaster Amazon Redshift, pastikan pencatatan audit diaktifkan.
500.14 (a)	(a) menerapkan kebijakan, prosedur, dan kontrol berbasis risiko yang dirancang untuk memantau aktivitas Pengguna Resmi dan mendeteksi akses atau penggunaan yang tidak sah, atau merusak, Informasi Nonpublik oleh Pengguna Resmi tersebut.	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.14 (b)	Sebagai bagian dari program keamanan siber, setiap entitas yang dilindungi harus: (b) memberikan pelatihan kesadaran keamanan siber reguler untuk semua personel yang diperbarui untuk mencerminkan risiko yang diidentifikasi oleh entitas yang tercakup dalam penilaian risikonya.	security-awareness -program-exists (pemeriksaan proses)	Membangun dan memelihara program kesadaran keamanan untuk organisas i Anda. Program kesadaran keamanan mendidik karyawan tentang cara melindungi organisas i mereka dari berbagai pelanggaran atau insiden keamanan.
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalana n melalui jaringan eksternal maupun saat istirahat.	opensearch-encrypt ed-at-rest	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk domain OpenSearc h Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalanan melalui jaringan eksternal maupun saat istirahat.	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalanan melalui jaringan eksternal maupun saat istirahat.	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalana n melalui jaringan eksternal maupun saat istirahat.	alb-http-to-https-pemeriksaan-pengalihan	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalana n melalui jaringan eksternal maupun saat istirahat.	api-gw-cache-enabl ed-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalana n melalui jaringan eksternal maupun saat istirahat.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrai l jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalana n melalui jaringan eksternal maupun saat istirahat.	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalana n melalui jaringan eksternal maupun saat istirahat.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalanan melalui jaringan eksternal maupun saat istirahat.	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalana n melalui jaringan eksternal maupun saat istirahat.	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalana n melalui jaringan eksternal maupun saat istirahat.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalana n melalui jaringan eksternal maupun saat istirahat.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalanan melalui jaringan eksternal maupun saat istirahat.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalana n melalui jaringan eksternal maupun saat istirahat.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalana n melalui jaringan eksternal maupun saat istirahat.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalana n melalui jaringan eksternal maupun saat istirahat.	s3- bucket-ssl-request s-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalana n melalui jaringan eksternal maupun saat istirahat.	sagemaker-endpoint -configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalana n melalui jaringan eksternal maupun saat istirahat.	sagemaker-notebook -instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalana n melalui jaringan eksternal maupun saat istirahat.	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalana n melalui jaringan eksternal maupun saat istirahat.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalana n melalui jaringan eksternal maupun saat istirahat.	rds-snapshot-encry pted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalana n melalui jaringan eksternal maupun saat istirahat.	alb-http-drop-invalid-Header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalana n melalui jaringan eksternal maupun saat istirahat.	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-n ode enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkrip si memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalana n melalui jaringan eksternal maupun saat istirahat.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalana n melalui jaringan eksternal maupun saat istirahat.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalanan melalui jaringan eksternal maupun saat istirahat.	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalana n melalui jaringan eksternal maupun saat istirahat.	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalana n melalui jaringan eksternal maupun saat istirahat.	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalana n melalui jaringan eksternal maupun saat istirahat.	s3- default-encryption -kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalana n melalui jaringan eksternal maupun saat istirahat.	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalana n melalui jaringan eksternal maupun saat istirahat.	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalana n melalui jaringan eksternal maupun saat istirahat.	codebuild-project-artifact-encryption	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk AWS CodeBuild artefak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.15 (a)	(a) Sebagai bagian dari program keamanan sibernya, berdasarkan Penilaian Risiko, setiap Entitas yang Tercakup harus menerapkan kontrol, termasuk enkripsi, untuk melindungi Informasi Nonpublik yang disimpan atau dikirimkan oleh Entitas yang Tercakup baik dalam perjalanan melalui jaringan eksternal maupun saat istirahat.	kinesis-stream-encrypted	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
500.16	(a) Sebagai bagian dari program keamanan sibernya, setiap entitas yang tercakup harus membuat rencana respons insiden tertulis yang dirancang untuk segera menanggapi, dan memulihkan dari, peristiwa keamanan siber apa pun yang secara material mempengaruhi kerahasiaan, integrita s, atau ketersedi aan sistem informasi entitas yang tercakup atau fungsionalitas berkelanjutan dari setiap aspek bisnis atau operasi entitas yang tercakup.	response-plan-exists-maintained (pemeriks aan proses)	Memastikan rencana respons insiden dibuat, dipelihara, dan didistribusikan kepada personel yang bertanggung jawab.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk NYDFS 23.

Praktik Terbaik Operasional untuk NZISM 3.8

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan

kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara Manual Keamanan Informasi (NZISM) Biro Keamanan Komunikasi Pemerintah Selandia Baru (GCSB) 2022-09 Versi 3.8 dan aturan Konfigurasi Terkelola. AWS Setiap aturan Config berlaku untuk jenis AWS sumber daya tertentu, dan berhubungan dengan satu atau beberapa kontrol NZISM. Kontrol NZISM dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini. Hanya kontrol yang mewakili praktik yang direkomendasikan atau dasar untuk informasi yang diklasifikasikan DIBATASI dan di bawah ini yang termasuk dalam pemetaan.

Templat paket kesesuaian sampel ini berisi pemetaan ke kontrol dalam kerangka kerja NZISM, yang merupakan bagian integral dari kerangka Persyaratan Keamanan Pelindung (PSR) yang menetapkan harapan Pemerintah Selandia Baru untuk pengelolaan personel, informasi, dan keamanan fisik.

NZISM dilisensikan di bawah lisensi Creative Commons Attribution 4.0 Selandia Baru, tersedia di mons. https://creativecom org/licenses/by/4.0/. Informasi hak cipta dapat ditemukan di Manual Keamanan Informasi Selandia Baru NZISM | Hukum, Privasi, dan Hak Cipta.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1149	Keamanan perangkat lunak, Lingkungan Operasi Standar, Pengembangan mengeras SOEs (14.1.8.C.01.)	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.
1149	Keamanan perangkat lunak, Lingkungan Operasi Standar, Pengembangan mengeras SOEs (14.1.8.C.01.)	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1149	Keamanan perangkat lunak, Lingkungan Operasi Standar, Pengembangan mengeras SOEs (14.1.8.C.01.)	ecs-containers-non privileged	Kontrol ini memeriksa apakah parameter istimewa dalam definisi penampung Definisi Tugas Amazon ECS disetel ke true. Kontrol gagal jika parameter ini sama dengan benar. Kontrol ini hanya mengevaluasi revisi aktif terbaru dari definisi tugas Amazon ECS. Kami menyarankan Anda menghapus hak istimewa yang ditinggikan dari definisi tugas ECS Anda. Ketika parameter hak istimewa benar, wadah diberikan hak istimewa yang ditinggikan pada instance wadah host (mirip dengan pengguna root).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1149	Keamanan perangkat lunak, Lingkungan Operasi Standar, Pengembangan mengeras SOEs (14.1.8.C.01.)	ecs-containers-readonly-access	Kontrol ini memeriksa apakah kontainer Amazon ECS terbatas pada akses hanya-baca ke sistem file root yang dipasang. Kontrol ini gagal jika ReadonlyRootFilesystem parameter dalam definisi container definisi tugas Amazon ECS disetel ke false. Kontrol ini hanya mengevaluasi revisi aktif terbaru dari definisi tugas Amazon ECS. Mengaktifkan opsi ini mengurangi vektor serangan keamanan karena sistem file instance kontainer tidak dapat dirusak atau ditulis kecuali jika memiliki izin baca-tulis eksplisit pada folder dan direktori sistem file. Kontrol ini juga menganut prinsip hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1661	Keamanan perangkat lunak, Pengembangan Aplikasi Web, konten situs web agensi (14.5.6.C.01.)	cloudfront-default-root-object-dikonfigurasi	Kontrol ini memeriksa apakah CloudFront distribusi Amazon dikonfigurasi untuk mengembalikan objek tertentu yang merupakan objek root default. Kontrol gagal jika CloudFront distribusi tidak memiliki objek root default yang dikonfigurasi. Pengguna terkadang meminta URL root distribusi alih-alih objek dalam distribusi. Ketika ini terjadi, menentukan objek root default dapat membantu Anda menghindari mengekspos konten distribusi web Anda. Aturan ini harus diterapkan di wilayah us-east-1. Terapkan dengan parameter template DeployEdgeRules = true

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1667	Keamanan perangkat lunak, Pengembangan Aplikasi Web, Aplikasi Web (14.5.8.C.01.)	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration. Nilainya 90 hari.
1667	Keamanan perangkat lunak, Pengembangan Aplikasi Web, Aplikasi Web (14.5.8.C.01.)	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1841	Kontrol Akses dan Kata Sandi, Identifikasi, Otentikasi dan Kata Sandi, Metode untuk identifikasi dan otentikasi pengguna sistem (16.1.35.C.02.)	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna IAM. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna IAM.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1841	Kontrol Akses dan Kata Sandi, Identifikasi, Otentikasi dan Kata Sandi, Metode untuk identifikasi dan otentikasi pengguna sistem (16.1.35.C.02.)	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna IAM, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1841	Kontrol Akses dan Kata Sandi, Identifikasi, Otentikasi dan Kata Sandi, Metode untuk identifikasi dan otentikasi pengguna sistem (16.1.35.C.02.)	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam sebuah AWS akun. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden akun yang disusupi. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1841	Kontrol Akses dan Kata Sandi, Identifikasi, Otentikasi dan Kata Sandi, Metode untuk identifikasi dan otentikasi pengguna sistem (16.1.35.C.02.)	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam sebuah AWS akun. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden akun yang disusupi. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1847	Kontrol Akses dan Kata Sandi, Identifikasi, Otentikasi dan Kata Sandi, Melindungi data otentikasi dalam perjalanan (16.1.37.C.01.)	alb-http-to-https-pemeriksaan-pengalihan	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1847	Kontrol Akses dan Kata Sandi, Identifikasi, Otentikasi dan Kata Sandi, Melindungi data otentikasi dalam perjalanan (16.1.37.C.01.)	cloudfront-viewer-policy-https	Kontrol ini memeriksa apakah CloudFront distribusi Amazon mengharuskan pemirsa untuk menggunakan HTTPS secara langsung atau menggunakan pengalihan. Kontrol gagal jika ViewerProtocolPolicy disetel ke allow-all for defaultCacheBehavior atau untuk cacheBehaviors. HTTPS (TLS) dapat digunakan untuk membantu mencegah penyerang potensial menggunakan person-in-the-middle atau serangan serupa untuk menguping atau memanipulasi lalu lintas jaringan. Hanya koneksi terenkripsi melalui HTTPS (TLS) yang diizinkan. Aturan ini harus diterapkan di wilayah us-east-1. Terapkan dengan parameter template DeployEdgeRules = true

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1847	Kontrol Akses dan Kata Sandi, Identifikasi, Otentikasi dan Kata Sandi, Melindungi data otentikasi dalam perjalanan (16.1.37. C.01.)	elasticsearch-node-to-node-pemeriksaan enkripsi-	Kontrol ini memeriksa apakah domain Elasticsearch telah node-to-node mengaktifkan enkripsi. Kontrol ini gagal jika node-to-node enkripsi dinonaktifkan pada domain. HTTPS (TLS) dapat digunakan untuk membantu mencegah penyerang potensial menguping atau memanipulasi lalu lintas jaringan menggunakan atau serangan serupa. person-in-the-middle Hanya koneksi terenkripsi melalui HTTPS (TLS) yang diizinkan. Mengaktifkan node-to-node enkripsi untuk domain Elasticsearch memastikan bahwa komunikasi intra-cluster dienkripsi dalam perjalanan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1847	Kontrol Akses dan Kata Sandi, Identifikasi, Otentikasi dan Kata Sandi, Melindungi data otentikasi dalam perjalanan (16.1.37. C.01.)	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1847	Kontrol Akses dan Kata Sandi, Identifikasi, Otentikasi dan Kata Sandi, Melindungi data otentikasi dalam perjalanan (16.1.37. C.01.)	opensearch-node-to-node-pemeriksaan enkripsi-	Kontrol ini memeriksa apakah OpenSearch domain telah mengaktifkan node-to-node enkripsi. Kontrol ini gagal jika node-to-node enkripsi dinonaktifkan pada domain. HTTPS (TLS) dapat digunakan untuk membantu mencegah penyerang potensial menguping atau memanipulasi lalu lintas jaringan menggunakan atau serangan serupa. person-in-the-middle Hanya koneksi terenkripsi melalui HTTPS (TLS) yang diizinkan. Mengaktifkan node-to-node enkripsi untuk OpenSearch domain memastikan bahwa komunikasi intra-cluster dienkripsi dalam perjalanan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1858	Kontrol Akses dan Kata Sandi, Identifikasi, Otentikasi dan Kata Sandi, Kebijakan pemilihan kata sandi (16.1.40.C.02.)	iam-password-policy	HTTPS (TLS) dapat digunakan untuk membantu mencegah penyerang potensial menggunakan person-in-the-middle atau serangan serupa untuk menguping atau memanipulasi lalu lintas jaringan. Hanya koneksi terenkripsi melalui HTTPS (TLS) yang diizinkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1893	Kontrol Akses dan Kata Sandi, Identifikasi, Otentikasi dan Kata Sandi, Penangguhan akses (16.1.46.C.02.)	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini menetapkan maxCredentialUsageUsia hingga 30 hari.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1946	Kontrol Akses dan Kata Sandi, Akses Pengguna Istimewa, Penggunaan akun istimewa (16.3.5.C .02.)	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1946	Kontrol Akses dan Kata Sandi, Akses Pengguna Istimewa, Penggunaan akun istimewa (16.3.5.C .02.)	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebagai gantinya, buat dan gunakan AWS akun berbasis peran untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.
1998	Kontrol Akses dan Kata Sandi, Pencatatan Acara dan Audit, Memelihara log manajemen sistem (16.6.6.C.02.)	cloud-trail-cloud-watch-logs-diaktifkan	Anda harus mengonfigurasi CloudTrail dengan CloudWatch Log untuk memantau log jejak Anda dan diberi tahu saat aktivitas tertentu terjadi. Aturan ini memeriksa apakah AWS CloudTrail jejak dikonfigurasi untuk mengirim log ke CloudWatch log Amazon.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1998	Kontrol Akses dan Kata Sandi, Pencatatan Acara dan Audit, Memelihara log manajemen sistem (16.6.6.C.02.)	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan AWS akun yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1998	Kontrol Akses dan Kata Sandi, Pencatatan Acara dan Audit, Memelihara log manajemen sistem (16.6.6.C.02.)	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya. Retensi minimum adalah 18 bulan.
2013	Kontrol Akses dan Kata Sandi, Pencatatan dan Audit Peristiwa, Peristiwa tambahan yang akan dicatat (16.6.10.C.02.)	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2013	Kontrol Akses dan Kata Sandi, Pencatatan dan Audit Peristiwa, Peristiwa tambahan yang akan dicatat (16.6.10.C.02.)	cloudfront-accesslogs-enabled	Kontrol ini memeriksa apakah pencatatan akses server diaktifkan pada CloudFront distribusi. Kontrol gagal jika pencatatan akses tidak diaktifkan untuk distribusi. CloudFront log akses memberikan informasi rinci tentang setiap permintaan pengguna yang CloudFront menerima. Setiap log berisi informasi seperti tanggal dan waktu permintaan diterima, alamat IP penampil yang membuat permintaan, sumber permintaan, dan nomor port permintaan dari penampil. Log ini berguna untuk aplikasi seperti audit keamanan dan akses dan investigasi forensik. Aturan ini harus diterapkan di wilayah us-east-1. Terapkan dengan parameter template

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			DeployEdgeRules = true
2013	Kontrol Akses dan Kata Sandi, Pencatatan dan Audit Peristiwa, Peristiwa tambahan yang akan dicatat (16.6.10.C.02.)	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan AWS akun yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2013	Kontrol Akses dan Kata Sandi, Pencatatan dan Audit Peristiwa, Peristiwa tambahan yang akan dicatat (16.6.10.C.02.)	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2013	Kontrol Akses dan Kata Sandi, Pencatatan dan Audit Peristiwa, Peristiwa tambahan yang akan dicatat (16.6.10.C.02.)	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2013	Kontrol Akses dan Kata Sandi, Pencatatan dan Audit Peristiwa, Peristiwa tambahan yang akan dicatat (16.6.10.C.02.)	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2022	Kontrol Akses dan Kata Sandi, Pencatatan dan Audit Peristiwa, Perlindungan log peristiwa (16.6.12.C.01.)	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.
2022	Kontrol Akses dan Kata Sandi, Pencatatan dan Audit Peristiwa, Perlindungan log peristiwa (16.6.12.C.01.)	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2028	Kontrol Akses dan Kata Sandi, Pencatatan dan Audit Acara, arsip log peristiwa (16.6.13.C.01.)	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya. Retensi minimum adalah 18 bulan.
2082	Kriptografi, Dasar-dasar Kriptografi, Mengurangi penyimpanan dan persyaratan transfer fisik (17.1.53.C.04.)	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Pengecualian tersedia untuk lingkungan pra-produksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2082	Kriptografi, Dasar-dasar Kriptogra fi, Mengurangi penyimpanan dan persyaratan transfer fisik (17.1.53.C.04.)	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrai l jejak Anda.
2082	Kriptografi, Dasar-dasar Kriptogra fi, Mengurangi penyimpanan dan persyaratan transfer fisik (17.1.53.C.04.)	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
2082	Kriptografi, Dasar-dasar Kriptogra fi, Mengurangi penyimpanan dan persyaratan transfer fisik (17.1.53.C.04.)	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2082	Kriptografi, Dasar-dasar Kriptogra fi, Mengurangi penyimpanan dan persyaratan transfer fisik (17.1.53.C.04.)	elasticsearch-encr ypted-at-rest	Kontrol ini memeriksa apakah domain Elasticsearch mengaktifkan konfigurasi. encryptio n-at-rest Pemeriksa an gagal jika enkripsi saat istirahat tidak diaktifkan. Untuk lapisan keamanan tambahan untuk data sensitif, Anda harus mengonfig urasi domain Layanan Elasticsearch Anda untuk dienkripsi saat istirahat. Saat Anda mengonfig urasi enkripsi data saat istirahat, AWS KMS menyimpan dan mengelola kunci enkripsi Anda. Untuk melakukan enkripsi, AWS KMS menggunakan algoritma Advanced Encryption Standard dengan kunci 256-bit (AES-256).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2082	Kriptografi, Dasar-dasar Kriptogra fi, Mengurangi penyimpanan dan persyaratan transfer fisik (17.1.53.C.04.)	volume terenkripsi	Karena data senstif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2082	Kriptografi, Dasar-dasar Kriptografi, Mengurangi penyimpanan dan persyaratan transfer fisik (17.1.53.C.04.)	opensearch-encrypted-at-rest	Kontrol ini memeriksa apakah OpenSearch domain memiliki encryption-at-rest konfigurasi yang diaktifkan. Pemeriksaan gagal jika enkripsi saat istirahat tidak diaktifkan. Untuk lapisan keamanan tambahan untuk data sensitif, Anda harus mengonfigurasi domain OpenSearch Layanan Anda untuk dienkripsi saat istirahat. Saat Anda mengonfigurasi enkripsi data saat istirahat, AWS KMS menyimpan dan mengelola kunci enkripsi Anda. Untuk melakukan enkripsi, AWS KMS menggunakan algoritma Advanced Encryption Standard dengan kunci 256-bit (AES-256).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2082	Kriptografi, Dasar-dasar Kriptografi, Mengurangi penyimpanan dan persyaratan transfer fisik (17.1.53.C.04.)	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
2082	Kriptografi, Dasar-dasar Kriptografi, Mengurangi penyimpanan dan persyaratan transfer fisik (17.1.53.C.04.)	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2082	Kriptografi, Dasar-dasar Kriptogra fi, Mengurangi penyimpanan dan persyaratan transfer fisik (17.1.53.C.04.)	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2082	Kriptografi, Dasar-dasar Kriptografi, Mengurangi penyimpanan dan persyaratan transfer fisik (17.1.53.C.04.)	s3- default-encryption-kms	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket S3 Anda. Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Untuk informasi lebih lanjut tentang proses enkripsi dan administrasi, gunakan AWS Key Management Service (AWS KMS) yang dikelola pelanggan CMKs. Pengecualian tersedia untuk bucket yang berisi data non-sensitif asalkan SSE diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2090	Kriptografi, Dasar-dasar Kriptografi, Perlindungan Informasi dan Sistem (17.1.55.C.02.)	alb-http-to-https-pemeriksaan-pengalihan	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
2090	Kriptografi, Dasar-dasar Kriptografi, Perlindungan Informasi dan Sistem (17.1.55.C.02.)	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2090	Kriptografi, Dasar-dasar Kriptogra fi, Perlindungan Informasi dan Sistem (17.1.55.C.02.)	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2598	Kriptografi, Keamanan Lapisan Transportasi, Menggunakan TLS (17.4.16.C.01.)	elb-custom-security-policy-ssl-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan pendengar ElasticLoadBalance r SSL Klasik Anda menggunakan kebijakan keamanan khusus. Kebijakan ini dapat menyediakan berbagai algoritma kriptografi berkekuat an tinggi untuk membantu memastika n komunikasi jaringan terenkripsi antar sistem. Aturan ini mengharuskan Anda menetapkan kebijakan keamanan khusus untuk pendengar SSL Anda. Kebijakan keamanann ya adalah: Protokol-TLSv1 .2, ECDHE-ECDSA- -GCM-. AES128 SHA256

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2600	Kriptografi, Keamanan Lapisan Transportasi, Menggunakan TLS (17.4.16.C.02.)	elb-custom-security-policy-ssl-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan pendengar ElasticLoadBalance r SSL Klasik Anda menggunakan kebijakan keamanan khusus. Kebijakan ini dapat menyediakan berbagai algoritma kriptografi berkekuat an tinggi untuk membantu memastika n komunikasi jaringan terenkripsi antar sistem. Aturan ini mengharuskan Anda menetapkan kebijakan keamanan khusus untuk pendengar SSL Anda. Kebijakan keamanan default adalah: Protocol-TLSv1 .2, ECDHE-ECDSA- -GCM-. AES128 SHA256

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2726	Kriptografi, Secure Shell, Akses jarak jauh otomatis (17.5.8.C.02.)	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3021	Kriptografi, Manajemen Kunci, Isi KMPs (17.9.25.C.01.)	cmk-backing-key-rotation-diaktifkan	AWS KMS memungkinkan pelanggan untuk memutar kunci dukungan, yang merupakan bahan kunci yang disimpan di AWS KMS dan terikat ke ID kunci CMK. Ini adalah kunci pendukung yang digunakan untuk melakukan operasi kriptografi seperti enkripsi dan dekripsi. Rotasi kunci otomatis saat ini mempertahankan semua kunci pendukung sebelumnya sehingga dekripsi data terenkripsi dapat berlangsung secara transparan. Memutar kunci enkripsi membantu mengurangi dampak potensial dari kunci yang dikompromikan karena data yang dienkripsi dengan kunci baru tidak dapat diakses dengan kunci sebelumnya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			yang mungkin telah diekspos.
3205	Keamanan jaringan, Manajemen Jaringan, Membatasi akses jaringan (18.1.13. C.02.)	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/ 0) akses jarak jauh dapat dikontrol ke sistem internal. Daftar port Internet resmi adalah: 443 saja

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3449	Keamanan Produk, Penambalan dan Pembaruan Produk, Menambal kerentanan dalam produk (12.4.4.C.02.)	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3449	Keamanan Produk, Penambalan dan Pembaruan Produk, Menambal kerentana n dalam produk (12.4.4.C.02.)	ecr-private-image-scanning-diaktifkan	Kontrol ini memeriksa apakah repositori ECR pribadi memiliki pemindaian gambar yang dikonfigurasi. Kontrol ini gagal jika repositori ECR pribadi tidak memiliki pemindaian gambar yang dikonfigurasi. Perhatikan bahwa Anda juga harus mengonfigurasi pemindaian pada push untuk setiap repositori untuk melewati kontrol ini. Pemindaian gambar ECR membantu mengidentifikasi kerentanan perangkat lunak dalam gambar kontainer Anda. ECR menggunakan database Common Vulnerabilities and Exposures (CVEs) dari proyek Clair open-source dan menyediakan daftar temuan pemindaia n. Mengaktifkan pemindaian gambar pada repositori

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			ECR menambahkan lapisan verifikasi untuk integritas dan keamanan gambar yang disimpan.
3449	Keamanan Produk, Penambalan dan Pembaruan Produk, Menambal kerentanan dalam produk (12.4.4.C.02.)	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini ditetapkan allowVersionUpgrade ke TRUE.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3451	Keamanan Produk, Penambalan dan Pembaruan Produk, Menambal kerentanan pada produk (12.4.4.C.04.)	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
3452	Keamanan Produk, Penambalan dan Pembaruan Produk, Menambal kerentanan dalam produk (12.4.4.C.05.)	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3452	Keamanan Produk, Penambalan dan Pembaruan Produk, Menambal kerentanan dalam produk (12.4.4.C.05.)	elastic-beanstalk-managed-updates-diaktifkan	Kontrol ini memeriksa apakah pembaruan platform terkelola diaktifkan untuk lingkungan Elastic Beanstalk. Mengaktifkan pembaruan platform terkelola memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah langkah penting dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3452	Keamanan Produk, Penambalan dan Pembaruan Produk, Menambal kerentanan dalam produk (12.4.4.C.05.)	rds-automatic-minor-version-upgrade diaktifkan	Kontrol ini memeriksa apakah upgrade versi minor otomatis diaktifkan untuk instance database RDS. Mengaktifkan upgrade versi minor otomatis memastikan bahwa pembaruan versi minor terbaru ke sistem manajemen basis data relasional (RDBMS) diinstal. Upgrade ini mungkin termasuk patch keamanan dan perbaikan bug. Tetap up to date dengan instalasi patch adalah langkah penting dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3453	Keamanan Produk, Penambalan dan Pembaruan Produk, Menambal kerentanan dalam produk (12.4.4.C.06.)	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
3453	Keamanan Produk, Penambalan dan Pembaruan Produk, Menambal kerentanan dalam produk (12.4.4.C.06.)	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini ditetapkan allowVersionUpgrade ke TRUE.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3562	Keamanan gateway, Gateway, Konfigura si gateway (19.1.12. C.01.)	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda. Pengecualian tersedia jika penyeimbang beban adalah asal untuk CloudFron t distribusi dengan WAF diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3562	Keamanan gateway, Gateway, Konfigurasi gateway (19.1.12.C.01.)	api-gw-associated-with-waf	Kontrol ini memeriksa apakah tahap API Gateway menggunakan daftar kontrol akses web AWS WAF (ACL). Kontrol ini gagal jika ACL web Regional AWS WAF tidak dilampirkan ke tahap REST API Gateway. AWS WAF adalah firewall aplikasi web yang membantu melindungi aplikasi web dan APIs dari serangan. Ini memungkinkan Anda untuk mengonfigurasi ACL, yang merupakan seperangkat aturan yang memungkinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap API Gateway Anda dikaitkan dengan ACL web AWS WAF untuk membantu melindunginya dari

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			serangan berbahaya. Pengecualian tersedia jika API Gateway adalah asal untuk CloudFront distribusi dengan WAF diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3562	Keamanan gateway, Gateway, Konfigura si gateway (19.1.12. C.01.)	cloudfront-associated-with-waf	Kontrol ini memeriksa apakah CloudFron t distribusi terkait dengan AWS WAF atau AWS WAFv2 web. ACLs Kontrol gagal jika distribusi tidak terkait dengan ACL web. AWS WAF adalah firewall aplikasi web yang membantu melindungi aplikasi web dan APIs dari serangan. Ini memungkinkan Anda untuk mengonfig urasi seperangkat aturan, yang disebut daftar kontrol akses web (web ACL), yang memungkin kan, memblokir, atau menghitung permintaa n web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan CloudFron t distribusi Anda dikaitkan dengan ACL web AWS WAF untuk membantu melindung inya dari serangan

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			berbahaya. Aturan ini harus diterapkan di wilayah us-east-1 . Terapkan dengan parameter template DeployEdgeRules = true
3562	Keamanan gateway, Gateway, Konfigura si gateway (19.1.12. C.01.)	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3562	Keamanan gateway, Gateway, Konfigura si gateway (19.1.12. C.01.)	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifka n untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.
3562	Keamanan gateway, Gateway, Konfigura si gateway (19.1.12. C.01.)	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3562	Keamanan gateway, Gateway, Konfigura si gateway (19.1.12. C.01.)	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3562	Keamanan gateway, Gateway, Konfigurasi gateway (19.1.12.C.01.)	elasticsearch-in-vpc-only	Kontrol ini memeriksa apakah domain Elasticsearch ada di VPC. Itu tidak mengevaluasi konfigurasi perutean subnet VPC untuk menentukan akses publik. Anda harus memastikan bahwa domain Elasticsearch tidak dilampirkan ke subnet publik. Domain Elasticsearch yang digunakan dalam VPC dapat berkomunikasi dengan sumber daya VPC melalui jaringan AWS pribadi, tanpa perlu melintasi internet publik. Konfigurasi ini meningkatkan postur keamanan dengan membatasi akses ke data dalam perjalanan. VPCs menyediakan sejumlah kontrol jaringan untuk mengamankan akses ke domain Elasticsearch, termasuk ACL jaringan dan grup keamanan

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3562	Keamanan gateway, Gateway, Konfigurasi gateway (19.1.12.C.01.)	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
3562	Keamanan gateway, Gateway, Konfigurasi gateway (19.1.12.C.01.)	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3562	Keamanan gateway, Gateway, Konfigurasi gateway (19.1.12.C.01.)	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3562	Keamanan gateway, Gateway, Konfigurasi gateway (19.1.12.C.01.)	opensearch-in-vpc-only	Kontrol ini memeriksa apakah OpenSearch domain berada dalam VPC. Itu tidak mengevaluasi konfigurasi perutean subnet VPC untuk menentukan akses publik. Anda harus memastikan bahwa OpenSearch domain tidak dilampirkan ke subnet publik. OpenSearch domain yang digunakan dalam VPC dapat berkomunikasi dengan sumber daya VPC melalui AWS jaringan pribadi, tanpa perlu melintasi internet publik. Konfigurasi ini meningkatkan postur keamanan dengan membatasi akses ke data dalam perjalanan. VPCs menyediakan sejumlah kontrol jaringan untuk mengamankan akses ke OpenSearch domain, termasuk

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			ACL jaringan dan grup keamanan.
3562	Keamanan gateway, Gateway, Konfigurasi gateway (19.1.12.C.01.)	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
3562	Keamanan gateway, Gateway, Konfigurasi gateway (19.1.12.C.01.)	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3562	Keamanan gateway, Gateway, Konfigurasi gateway (19.1.12.C.01.)	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini ditetapkan ignorePublicAcls ke TRUE, blockPublicPolicy TRUE, blockPublicAcls TRUE, dan restrictPublicBuckets TRUE.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3562	Keamanan gateway, Gateway, Konfigurasi gateway (19.1.12.C.01.)	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3562	Keamanan gateway, Gateway, Konfigura si gateway (19.1.12. C.01.)	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3562	Keamanan gateway, Gateway, Konfigura si gateway (19.1.12. C.01.)	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3623	Keamanan gerbang, Gateway, zona demiliterisasi (19.1.14.C.02.)	elasticsearch-in-vpc-only	Kontrol ini memeriksa apakah domain Elasticsearch ada di VPC. Itu tidak mengevaluasi konfigurasi perutean subnet VPC untuk menentukan akses publik. Anda harus memastikan bahwa domain Elasticsearch tidak dilampirkan ke subnet publik. Domain Elasticsearch yang digunakan dalam VPC dapat berkomunikasi dengan sumber daya VPC melalui jaringan AWS pribadi, tanpa perlu melintasi internet publik. Konfigurasi ini meningkatkan postur keamanan dengan membatasi akses ke data dalam perjalanan. VPCs menyediakan sejumlah kontrol jaringan untuk mengamankan akses ke domain Elasticsearch, termasuk ACL jaringan dan grup keamanan

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3623	Keamanan gerbang, Gateway, zona demiliterisasi (19.1.14.C.02.)	opensearch-in-vpc-only	Kontrol ini memeriksa apakah OpenSearch domain berada dalam VPC. Itu tidak mengevaluasi konfigurasi perutean subnet VPC untuk menentukan akses publik. Anda harus memastikan bahwa OpenSearch domain tidak dilampirkan ke subnet publik. OpenSearch domain yang digunakan dalam VPC dapat berkomunikasi dengan sumber daya VPC melalui AWS jaringan pribadi, tanpa perlu melintasi internet publik. Konfigurasi ini meningkatkan postur keamanan dengan membatasi akses ke data dalam perjalanan. VPCs menyediakan sejumlah kontrol jaringan untuk mengamankan akses ke OpenSearch domain, termasuk

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			ACL jaringan dan grup keamanan.
3623	Keamanan gerbang, Gateway, zona demiliterisasi (19.1.14.C.02.)	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
3623	Keamanan gerbang, Gateway, zona demiliterisasi (19.1.14.C.02.)	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3815	Keamanan jaringan, Deteksi dan Pencegahan Intrusi, Pemeliharaan IDS/IPS (18.4.9.C.01.)	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3857	Keamanan jaringan, Deteksi dan Pencegahan Intrusi, Mengkonfigurasi IDS/IPS (18.4.11.C.01.)	guardduty-eks-protection-audit-diaktifkan	Kontrol ini memeriksa apakah Pemantauan Log Audit GuardDuty EKS diaktifkan. GuardDuty Pemantauan Log Audit EKS membantu Anda mendeteksi aktivitas yang berpotensi mencurigakan di kluster Amazon Elastic Kubernetes Service (Amazon EKS). EKS Audit Log Monitoring menggunakan log audit Kubernetes untuk menangkap aktivitas kronologis dari pengguna, aplikasi yang menggunakan Kubernetes API, dan control plane.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3857	Keamanan jaringan, Deteksi dan Pencegahan Intrusi, Mengkonfigurasi IDS/IPS (18.4.11.C.01.)	guardduty-eks-protection-runtime-diaktifkan	Kontrol ini memeriksa apakah GuardDuty EKS Runtime Monitoring dengan manajemen agen otomatis diaktifkan. Perlindungan EKS di Amazon GuardDuty menyediakan cakupan deteksi ancaman untuk membantu Anda melindungi kluster Amazon EKS di AWS lingkungan Anda. EKS Runtime Monitoring menggunakan peristiwa tingkat sistem operasi untuk membantu Anda mendeteksi potensi ancaman di node dan kontainer EKS dalam kluster EKS Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3857	Keamanan jaringan, Deteksi dan Pencegahan Intrusi, Mengkonfigurasi IDS/IPS (18.4.11.C.01.)	guardduty-lambda-protection-enabled	Kontrol ini memeriksa apakah Perlindungan GuardDuty Lambda diaktifkan. GuardDuty Perlindungan Lambda membantu Anda mengidentifikasi potensi ancaman keamanan saat fungsi AWS Lambda dipanggil. Setelah Anda mengaktif kan Perlindungan Lambda, GuardDuty mulai memantau log aktivitas jaringan Lambda yang terkait dengan fungsi Lambda di akun Anda. AWS Ketika fungsi Lambda dipanggil dan GuardDuty mengident ifikasi lalu lintas jaringan mencuriga kan yang menunjukk an adanya potongan kode yang berpotens i berbahaya dalam fungsi Lambda Anda, menghasilkan temuan. GuardDuty

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3857	Keamanan jaringan, Deteksi dan Pencegahan Intrusi, Mengkonfigurasi IDS/IPS (18.4.11.C.01.)	guardduty-s3-protection-enabled	Kontrol ini memeriksa apakah Perlindungan GuardDuty S3 diaktifkan. Perlindungan S3 memungkinkan GuardDuty untuk memantau operasi API tingkat objek untuk mengidentifikasi potensi risiko keamanan untuk data dalam bucket Amazon S3 Anda. GuardDuty memantau ancaman terhadap sumber daya S3 Anda dengan menganalisis peristiwa AWS CloudTrail manajemen dan peristiwa data CloudTrail S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3875	Keamanan jaringan, Deteksi dan Pencegahan Intrusi, Manajemen dan korelasi peristiwa (18.4.12.C.01.)	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3875	Keamanan jaringan, Deteksi dan Pencegahan Intrusi, Manajemen dan korelasi peristiwa (18.4.12.C.01.)	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4333	Manajemen data, Penyaringan Konten, Validasi konten (20.3.7.C.02.)	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4333	Manajemen data, Penyaringan Konten, Validasi konten (20.3.7.C.02.)	api-gw-associated-with-waf	Kontrol ini memeriksa apakah tahap API Gateway menggunakan daftar kontrol akses web AWS WAF (ACL). Kontrol ini gagal jika ACL web Regional AWS WAF tidak dilampirkan ke tahap REST API Gateway. AWS WAF adalah firewall aplikasi web yang membantu melindungi aplikasi web dan APIs dari serangan. Ini memungkinkan Anda untuk mengonfigurasi ACL, yang merupakan seperangkat aturan yang memungkinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap API Gateway Anda dikaitkan dengan ACL web AWS WAF untuk membantu melindunginya dari

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			serangan berbahaya. Pengecualian tersedia jika API Gateway adalah asal untuk CloudFront distribusi dengan WAF diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4441	Manajemen data, Database, file Database (20.4.4.C .02.)	elasticsearch-encrypted-at-rest	Kontrol ini memeriksa apakah domain Elasticsearch mengaktifkan konfigurasi. encryption-at-rest Pemeriksaan gagal jika enkripsi saat istirahat tidak diaktifkan. Untuk lapisan keamanan tambahan untuk data sensitif, Anda harus mengonfigurasi domain Layanan Elasticsearch Anda untuk dienkripsi saat istirahat. Saat Anda mengonfigurasi enkripsi data saat istirahat, AWS KMS menyimpan dan mengelola kunci enkripsi Anda. Untuk melakukan enkripsi, AWS KMS menggunakan algoritma Advanced Encryption Standard dengan kunci 256-bit (AES-256).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4441	Manajemen data, Database, file Database (20.4.4.C .02.)	opensearch-encrypted-at-rest	Kontrol ini memeriksa apakah OpenSearch domain memiliki encryption-at-rest konfigurasi yang diaktifkan. Pemeriksaan gagal jika enkripsi saat istirahat tidak diaktifkan. Untuk lapisan keamanan tambahan untuk data sensitif, Anda harus mengonfigurasi domain OpenSearch Layanan Anda untuk dienkripsi saat istirahat. Saat Anda mengonfigurasi enkripsi data saat istirahat, AWS KMS menyimpan dan mengelola kunci enkripsi Anda. Untuk melakukan enkripsi, AWS KMS menggunakan algoritma Advanced Encryption Standard dengan kunci 256-bit (AES-256).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4441	Manajemen data, Database, file Database (20.4.4.C .02.)	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
4441	Manajemen data, Database, file Database (20.4.4.C .02.)	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4441	Manajemen data, Database, file Database (20.4.4.C .02.)	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
4441	Manajemen data, Database, file Database (20.4.4.C .02.)	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4441	Manajemen data, Database, file Database (20.4.4.C .02.)	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini disetel clusterDbEncrypted ke TRUE, dan LoggingEnabled ke TRUE.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4445	Manajemen data, Database, Akuntabilitas (20.4.5.C.02.)	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4445	Manajemen data, Database, Akuntabilitas (20.4.5.C.02.)	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini disetel clusterDbEncrypted ke TRUE, dan LoggingEnabled ke TRUE.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4829	Keamanan sistem perusahaan, Komputasi Awan, Ketersediaan Sistem (22.1.23.C.01.)	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4829	Keamanan sistem perusahaan, Komputasi Awan, Ketersediaan Sistem (22.1.23.C.01.)	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4829	Keamanan sistem perusahaan, Komputasi Awan, Ketersediaan Sistem (22.1.23.C.01.)	rds-cluster-multi-az-diaktifkan	Amazon Aurora menyimpan salinan data dalam cluster DB di beberapa Availability Zone dalam satu AWS Wilayah. Aurora menyimpan salinan ini terlepas jika instans dalam klaster DB mencakup beberapa Zona Ketersediaan. Ketika data ditulis ke instans DB primer, Aurora secara sinkron mereplikasi data di seluruh Zona Ketersediaan ke enam simpul penyimpanan yang terkait dengan volume klaster Anda. Melakukan hal tersebut akan memberikan redundansi data, menghilangkan I/O freeze, dan meminimalkan lonjakan latensi selama pencadangan sistem. Menjalankan instans DB dengan ketersediaan tinggi dapat meningkat

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			kan ketersediaan selama pemeliharaan sistem terencana, dan membantu melindung i basis data Anda terhadap kegagalan dan gangguan Zona Ketersediaan. Aturan ini memeriksa apakah replikasi Multi-AZ diaktifkan di klaster Amazon Aurora yang dikelola oleh Amazon RDS. Pengecual ian tersedia untuk lingkungan pra-produ ksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4829	Keamanan sistem perusahaan, Komputasi Awan, Ketersediaan Sistem (22.1.23.C.01.)	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			Pengecualian tersedia untuk lingkungan pra-produksi.
4838	Keamanan sistem perusahaan, Komputasi Awan, Akses Tidak Sah (22.1.24.C.03.)	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup informasi AWS akun yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
4838	Keamanan sistem perusahaan, Komputasi Awan, Akses Tidak Sah (22.1.24.C.03.)	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4838	Keamanan sistem perusahaan, Komputasi Awan, Akses Tidak Sah (22.1.24.C.03.)	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini ditetapkan ignorePublicAcls ke TRUE, blockPublicPolicy TRUE, blockPublicAcls TRUE, dan restrictPublicBuckets TRUE.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4838	Keamanan sistem perusahaan, Komputasi Awan, Akses Tidak Sah (22.1.24.C.03.)	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
4838	Keamanan sistem perusahaan, Komputasi Awan, Akses Tidak Sah (22.1.24.C.03.)	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4839	Keamanan sistem perusahaan, Komputasi Awan, Akses Tidak Sah (22.1.24.C.04.)	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
4839	Keamanan sistem perusahaan, Komputasi Awan, Akses Tidak Sah (22.1.24.C.04.)	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4839	Keamanan sistem perusahaan, Komputasi Awan, Akses Tidak Sah (22.1.24.C.04.)	elasticsearch-encrypted-at-rest	Kontrol ini memeriksa apakah domain Elasticsearch mengaktifkan konfigurasi. encryption-at-rest Pemeriksaan gagal jika enkripsi saat istirahat tidak diaktifkan. Untuk lapisan keamanan tambahan untuk data sensitif, Anda harus mengonfigurasi domain Layanan Elasticsearch Anda untuk dienkripsi saat istirahat. Saat Anda mengonfigurasi enkripsi data saat istirahat, AWS KMS menyimpan dan mengelola kunci enkripsi Anda. Untuk melakukan enkripsi, AWS KMS menggunakan algoritma Advanced Encryption Standard dengan kunci 256-bit (AES-256).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4839	Keamanan sistem perusahaan, Komputasi Awan, Akses Tidak Sah (22.1.24.C.04.)	elasticsearch-node-to-node-pemeriksaan enkripsi-	Kontrol ini memeriksa apakah domain Elasticsearch telah node-to-node mengaktifkan enkripsi. Kontrol ini gagal jika node-to-node enkripsi dinonaktifkan pada domain. HTTPS (TLS) dapat digunakan untuk membantu mencegah penyerang potensial menguping atau memanipulasi lalu lintas jaringan menggunakan atau serangan serupa. person-in-the-midd le Hanya koneksi terenkripsi melalui HTTPS (TLS) yang diizinkan. Mengaktif kan node-to-n ode enkripsi untuk domain Elasticsearch memastikan bahwa komunikasi intra-clu ster dienkripsi dalam perjalanan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4839	Keamanan sistem perusahaan, Komputasi Awan, Akses Tidak Sah (22.1.24.C.04.)	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
4839	Keamanan sistem perusahaan, Komputasi Awan, Akses Tidak Sah (22.1.24.C.04.)	volume terenkripsi	Karena data senstif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4839	Keamanan sistem perusahaan, Komputasi Awan, Akses Tidak Sah (22.1.24.C.04.)	opensearch-encrypted-at-rest	Kontrol ini memeriksa apakah OpenSearch domain memiliki encryption-at-rest konfigurasi yang diaktifkan. Pemeriksaan gagal jika enkripsi saat istirahat tidak diaktifkan. Untuk lapisan keamanan tambahan untuk data sensitif, Anda harus mengonfigurasi domain OpenSearch Layanan Anda untuk dienkripsi saat istirahat. Saat Anda mengonfigurasi enkripsi data saat istirahat, AWS KMS menyimpan dan mengelola kunci enkripsi Anda. Untuk melakukan enkripsi, AWS KMS menggunakan algoritma Advanced Encryption Standard dengan kunci 256-bit (AES-256).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4839	Keamanan sistem perusahaan, Komputasi Awan, Akses Tidak Sah (22.1.24.C.04.)	opensearch-node-to-node-pemeriksaan enkripsi-	Kontrol ini memeriksa apakah OpenSearch domain telah mengaktifkan node-to-node enkripsi. Kontrol ini gagal jika node-to-node enkripsi dinonaktifkan pada domain. HTTPS (TLS) dapat digunakan untuk membantu mencegah penyerang potensial menguping atau memanipulasi lalu lintas jaringan menggunakan atau serangan serupa. person-in-the-middle Hanya koneksi terenkripsi melalui HTTPS (TLS) yang diizinkan. Mengaktifkan node-to-node enkripsi untuk OpenSearch domain memastikan bahwa komunikasi intra-cluster dienkripsi dalam perjalanan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4839	Keamanan sistem perusahaan, Komputasi Awan, Akses Tidak Sah (22.1.24.C.04.)	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
4839	Keamanan sistem perusahaan, Komputasi Awan, Akses Tidak Sah (22.1.24.C.04.)	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4839	Keamanan sistem perusahaan, Komputasi Awan, Akses Tidak Sah (22.1.24.C.04.)	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini disetel clusterDbEncrypted ke TRUE, dan LoggingEnabled ke TRUE.
4839	Keamanan sistem perusahaan, Komputasi Awan, Akses Tidak Sah (22.1.24.C.04.)	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4839	Keamanan sistem perusahaan, Komputasi Awan, Akses Tidak Sah (22.1.24.C.04.)	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
4839	Keamanan sistem perusahaan, Komputasi Awan, Akses Tidak Sah (22.1.24.C.04.)	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4839	Keamanan sistem perusahaan, Komputasi Awan, Akses Tidak Sah (22.1.24.C.04.)	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
4839	Keamanan sistem perusahaan, Komputasi Awan, Akses Tidak Sah (22.1.24.C.04.)	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4839	Keamanan sistem perusahaan, Komputasi Awan, Akses Tidak Sah (22.1.24.C.04.)	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunak an Key Managemen t Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublika sikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Pengecual ian tersedia ketika pesan yang dipublika sikan ke topik tidak mengandung data sensitif.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4849	Keamanan sistem perusahaan, Komputasi Awan, Pencadangan, Pengarsipan Pemulihan, dan Remanensi Data (22.1.26.C.01.)	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4849	Keamanan sistem perusahaan, Komputasi Awan, Pencadangan, Pengarsipan Pemulihan, dan Remanensi Data (22.1.26.C.01.)	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Pengecualian tersedia ketika solusi pemulihan kompensasi telah dikonfigurasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4849	Keamanan sistem perusahaan, Komputasi Awan, Pencadangan, Pengarsipan Pemulihan, dan Remanensi Data (22.1.26.C.01.)	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan cadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4849	Keamanan sistem perusahaan, Komputasi Awan, Pencadangan, Pengarsipan Pemulihan, dan Remanensi Data (22.1.26.C.01.)	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda. Pengecual ian tersedia ketika solusi pemulihan kompensasi telah dikonfigurasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4849	Keamanan sistem perusahaan, Komputasi Awan, Pencadangan, Pengarsipan Pemulihan, dan Remanensi Data (22.1.26.C.01.)	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Pengecualian tersedia ketika solusi pemulihan kompensasi telah dikonfigurasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4849	Keamanan sistem perusahaan, Komputasi Awan, Pencadangan, Pengarsipan Pemulihan, dan Remanensi Data (22.1.26.C.01.)	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4849	Keamanan sistem perusahaan, Komputasi Awan, Pencadangan, Pengarsipan Pemulihan, dan Remanensi Data (22.1.26.C.01.)	rds-cluster-deletion-protection-diaktifkan	Pastikan instans Amazon RDS mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4849	Keamanan sistem perusahaan, Komputasi Awan, Pencadangan, Pengarsipan Pemulihan, dan Remanensi Data (22.1.26.C.01.)	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda. Pengecual ian tersedia ketika solusi pemulihan kompensasi telah dikonfigurasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4849	Keamanan sistem perusahaan, Komputasi Awan, Pencadangan, Pengarsipan Pemulihan, dan Remanensi Data (22.1.26.C.01.)	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4849	Keamanan sistem perusahaan, Komputasi Awan, Pencadangan, Pengarsipan Pemulihan, dan Remanensi Data (22.1.26.C.01.)	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk cluster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB per node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4849	Keamanan sistem perusahaan, Komputasi Awan, Pencadangan, Pengarsipan Pemulihan, dan Remanensi Data (22.1.26.C.01.)	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginka n dan kegagalan aplikasi. Pengecual ian tersedia ketika hanya satu varian objek yang akan dibuat, atau ketika solusi pemulihan kompensasi telah dikonfigurasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6843	Kontrol Akses dan Kata Sandi, Manajemen Akses Istimewa, Prinsip Hak Istimewa Paling Sedikit (16.4.31.C.02.)	mfa-enabled-for-iam-akses konsol	MFA menambahkan keamanan ekstra dengan mengharuskan pengguna untuk memberikan otentikasi unik dari mekanisme MFA yang didukung AWS - selain kredensyal masuk reguler mereka - ketika mereka mengakses situs web atau layanan. AWS Mekanisme yang didukung termasuk kunci keamanan U2F, perangkat MFA virtual atau perangkat keras, dan kode berbasis SMS. Aturan ini memeriksa apakah AWS Multi-Factor Authentication (MFA) diaktifkan untuk semua pengguna Identity and Access Management (IAM) and Access AWS Management (IAM) yang menggunakan kata sandi konsol. Aturannya sesuai jika MFA diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6843	Kontrol Akses dan Kata Sandi, Manajemen Akses Istimewa, Prinsip Hak Istimewa Paling Sedikit (16.4.31.C.02.)	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam sebuah AWS akun. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden akun yang disusupi. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6852	Kontrol Akses dan Kata Sandi, Manajemen Akses Istimewa, Penangguhan dan Pencabutan Kredensyal Akses Istimewa (16.4.33.C.01.)	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini menetapkan maxCredentialUsageUsia hingga 30 hari.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6860	Kontrol Akses dan Kata Sandi, Manajemen Akses Istimewa, Pemantauan dan Peninjauan (16.4.35.C.02.)	cloud-trail-cloud-watch-logs-diaktifkan	Anda harus mengonfigurasi CloudTrail dengan CloudWatch Log untuk memantau log jejak Anda dan diberi tahu saat aktivitas tertentu terjadi. Aturan ini memeriksa apakah AWS CloudTrail jejak dikonfigurasi untuk mengirim log ke CloudWatch log Amazon.
6860	Kontrol Akses dan Kata Sandi, Manajemen Akses Istimewa, Pemantauan dan Peninjauan (16.4.35.C.02.)	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan AWS akun yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6861	Kontrol Akses dan Kata Sandi, Manajemen Akses Istimewa, Pemantauan dan Peninjauan (16.4.35.C.03.)	cloudtrail-security-trail-enabled	Aturan ini membantu memastikan penggunaan praktik terbaik keamanan yang AWS direkomendasikan untuk AWS CloudTrail, dengan memeriksa pengaktifan beberapa pengaturan. Ini termasuk penggunaan enkripsi log, validasi log, dan mengaktifkan AWS CloudTrail di beberapa wilayah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6953	Kontrol Akses dan Kata Sandi, Otentikasi Multi-Faktor, Arsitektur Sistem dan Kontrol Keamanan (16.7.34.C.02.)	mfa-enabled-for-iam-akses konsol	MFA menambahkan keamanan ekstra dengan mengharuskan pengguna untuk memberikan otentikasi unik dari mekanisme MFA yang didukung AWS - selain kredensyal masuk reguler mereka - ketika mereka mengakses situs web atau layanan. AWS Mekanisme yang didukung termasuk kunci keamanan U2F, perangkat MFA virtual atau perangkat keras, dan kode berbasis SMS. Aturan ini memeriksa apakah AWS Multi-Factor Authentication (MFA) diaktifkan untuk semua pengguna Identity and Access Management (IAM) and Access AWS Management (IAM) yang menggunakan kata sandi konsol. Aturannya sesuai jika MFA diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6953	Kontrol Akses dan Kata Sandi, Otentikasi Multi-Faktor, Arsitektur Sistem dan Kontrol Keamanan (16.7.34. C.02.)	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam sebuah AWS akun. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden akun yang disusupi. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7436	Keamanan Cloud Publik, Manajemen Identitas dan Kontrol Akses, Nama Pengguna dan Kata Sandi (23.3.19.C.01.)	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna IAM. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna IAM.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7436	Keamanan Cloud Publik, Manajemen Identitas dan Kontrol Akses, Nama Pengguna dan Kata Sandi (23.3.19.C.01.)	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna IAM, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7436	Keamanan Cloud Publik, Manajemen Identitas dan Kontrol Akses, Nama Pengguna dan Kata Sandi (23.3.19.C.01.)	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam sebuah AWS akun. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden akun yang disusupi. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7436	Keamanan Cloud Publik, Manajemen Identitas dan Kontrol Akses, Nama Pengguna dan Kata Sandi (23.3.19.C.01.)	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam sebuah AWS akun. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden akun yang disusupi. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7437	Keamanan Cloud Publik, Manajemen Identitas dan Kontrol Akses, Nama Pengguna dan Kata Sandi (23.3.19.C.01.)	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna IAM. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna IAM.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7437	Keamanan Cloud Publik, Manajemen Identitas dan Kontrol Akses, Nama Pengguna dan Kata Sandi (23.3.19.C.01.)	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna IAM, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7437	Keamanan Cloud Publik, Manajemen Identitas dan Kontrol Akses, Nama Pengguna dan Kata Sandi (23.3.19.C.01.)	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam sebuah AWS akun. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden akun yang disusupi. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7437	Keamanan Cloud Publik, Manajemen Identitas dan Kontrol Akses, Nama Pengguna dan Kata Sandi (23.3.19.C.01.)	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam sebuah AWS akun. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden akun yang disusupi. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7466	Keamanan Cloud Publik, Perlindungan Data di Cloud Publik, Aksesibilitas Data (23.4.10.C.01.)	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7466	Keamanan Cloud Publik, Perlindungan Data di Cloud Publik, Aksesibilitas Data (23.4.10.C.01.)	api-gw-associated-with-waf	Kontrol ini memeriksa apakah tahap API Gateway menggunakan daftar kontrol akses web AWS WAF (ACL). Kontrol ini gagal jika ACL web Regional AWS WAF tidak dilampirkan ke tahap REST API Gateway. AWS WAF adalah firewall aplikasi web yang membantu melindungi aplikasi web dan APIs dari serangan. Ini memungkinkan Anda untuk mengonfigurasi ACL, yang merupakan seperangkat aturan yang memungkinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap API Gateway Anda dikaitkan dengan ACL web AWS WAF untuk membantu melindunginya dari

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			serangan berbahaya. Pengecualian tersedia jika API Gateway adalah asal untuk CloudFront distribusi dengan WAF diaktifkan.
7466	Keamanan Cloud Publik, Perlindungan Data di Cloud Publik, Aksesibilitas Data (23.4.10.C.01.)	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7466	Keamanan Cloud Publik, Perlindungan Data di Cloud Publik, Aksesibilitas Data (23.4.10.C.01.)	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifka n untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunakan kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.
7466	Keamanan Cloud Publik, Perlindungan Data di Cloud Publik, Aksesibilitas Data (23.4.10.C.01.)	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7466	Keamanan Cloud Publik, Perlindungan Data di Cloud Publik, Aksesibilitas Data (23.4.10.C.01.)	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7466	Keamanan Cloud Publik, Perlindungan Data di Cloud Publik, Aksesibilitas Data (23.4.10.C.01.)	elasticsearch-in-vpc-only	Kontrol ini memeriksa apakah domain Elasticsearch ada di VPC. Itu tidak mengevaluasi konfigurasi perutean subnet VPC untuk menentukan akses publik. Anda harus memastikan bahwa domain Elasticsearch tidak dilampirkan ke subnet publik. Domain Elasticsearch yang digunakan dalam VPC dapat berkomunikasi dengan sumber daya VPC melalui jaringan AWS pribadi, tanpa perlu melintasi internet publik. Konfigurasi ini meningkatkan postur keamanan dengan membatasi akses ke data dalam perjalanan. VPCs menyediakan sejumlah kontrol jaringan untuk mengamankan akses ke domain Elasticsearch, termasuk ACL jaringan dan grup keamanan

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7466	Keamanan Cloud Publik, Perlindungan Data di Cloud Publik, Aksesibilitas Data (23.4.10.C.01.)	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
7466	Keamanan Cloud Publik, Perlindungan Data di Cloud Publik, Aksesibilitas Data (23.4.10.C.01.)	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7466	Keamanan Cloud Publik, Perlindungan Data di Cloud Publik, Aksesibilitas Data (23.4.10.C.01.)	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7466	Keamanan Cloud Publik, Perlindungan Data di Cloud Publik, Aksesibilitas Data (23.4.10.C.01.)	opensearch-in-vpc-only	Kontrol ini memeriksa apakah OpenSearch domain berada dalam VPC. Itu tidak mengevaluasi konfigurasi perutean subnet VPC untuk menentukan akses publik. Anda harus memastikan bahwa OpenSearch domain tidak dilampirkan ke subnet publik. OpenSearch domain yang digunakan dalam VPC dapat berkomunikasi dengan sumber daya VPC melalui AWS jaringan pribadi, tanpa perlu melintasi internet publik. Konfigurasi ini meningkatkan postur keamanan dengan membatasi akses ke data dalam perjalanan. VPCs menyediakan sejumlah kontrol jaringan untuk mengamankan akses ke OpenSearch domain, termasuk

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			ACL jaringan dan grup keamanan.
7466	Keamanan Cloud Publik, Perlindungan Data di Cloud Publik, Aksesibilitas Data (23.4.10.C.01.)	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
7466	Keamanan Cloud Publik, Perlindungan Data di Cloud Publik, Aksesibilitas Data (23.4.10.C.01.)	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7466	Keamanan Cloud Publik, Perlindungan Data di Cloud Publik, Aksesibilitas Data (23.4.10.C.01.)	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini ditetapkan ignorePublicAcls ke TRUE, blockPublicPolicy TRUE, blockPublicAcls TRUE, dan restrictPublicBuckets TRUE.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7466	Keamanan Cloud Publik, Perlindungan Data di Cloud Publik, Aksesibilitas Data (23.4.10.C.01.)	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
7466	Keamanan Cloud Publik, Perlindungan Data di Cloud Publik, Aksesibilitas Data (23.4.10.C.01.)	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7466	Keamanan Cloud Publik, Perlindungan Data di Cloud Publik, Aksesibilitas Data (23.4.10.C.01.)	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7466	Keamanan Cloud Publik, Perlindungan Data di Cloud Publik, Aksesibilitas Data (23.4.10.C.01.)	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
7496	Keamanan Cloud Publik, Pencatatan, dan Peringatan di Cloud Publik, persyaratan Pencatatan (23.5.11.C.01.)	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7496	Keamanan Cloud Publik, Pencatatan, dan Peringatan di Cloud Publik, persyaratan Pencatatan (23.5.11.C.01.)	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7496	Keamanan Cloud Publik, Pencatatan, dan Peringatan di Cloud Publik, persyaratan Pencatatan (23.5.11.C.01.)	cloudfront-accesslogs-enabled	Kontrol ini memeriksa apakah pencatatan akses server diaktifkan pada CloudFront distribusi. Kontrol gagal jika pencatatan akses tidak diaktifkan untuk distribusi. CloudFront log akses memberikan informasi rinci tentang setiap permintaan pengguna yang CloudFront menerima. Setiap log berisi informasi seperti tanggal dan waktu permintaan diterima, alamat IP penampil yang membuat permintaan, sumber permintaan, dan nomor port permintaan dari penampil. Log ini berguna untuk aplikasi seperti audit keamanan dan akses dan investigasi forensik. Aturan ini harus diterapkan di wilayah us-east-1.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7496	Keamanan Cloud Publik, Pencatata n, dan Peringata n di Cloud Publik, persyaratan Pencatatan (23.5.11. C.01.)	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan AWS akun yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
7496	Keamanan Cloud Publik, Pencatata n, dan Peringata n di Cloud Publik, persyaratan Pencatatan (23.5.11. C.01.)	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7496	Keamanan Cloud Publik, Pencatatan, dan Peringatan di Cloud Publik, persyaratan Pencatatan (23.5.11.C.01.)	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7496	Keamanan Cloud Publik, Pencatata n, dan Peringata n di Cloud Publik, persyaratan Pencatatan (23.5.11. C.01.)	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7496	Keamanan Cloud Publik, Pencatatan, dan Peringatan di Cloud Publik, persyaratan Pencatatan (23.5.11.C.01.)	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk NZISM.

Praktik Terbaik Operasional untuk PCI DSS 3.2.1

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk

membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) 3.2.1 dan aturan Config terkelola AWS . Setiap AWS Config aturan berlaku untuk AWS sumber daya tertentu, dan berhubungan dengan satu atau lebih kontrol PCI DSS. Kontrol PCI DSS dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3	Melarang akses publik langsung antara Internet dan komponen sistem apa pun di lingkungan data pemegang kartu.	alb-desync-mode-check	Untuk membantu melindungi aplikasi untuk kerentanan HTTP Desync, pastikan mode mitigasi HTTP Desync diaktifkan pada penyeimbang beban aplikasi Anda. Masalah HTTP Desync dapat menyebabkan penyelundupan permintaan dan membuat aplikasi Anda rentan terhadap antrian permintaan atau keracunan cache. Mode mitigasi desync adalah monitor, defensif, dan paling ketat. Defensif adalah mode default.
1.3	Melarang akses publik langsung	alb-http-drop-invalid-Header-diaktifkan	Pastikan Elastic Load Balancers (ELB)

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	antara Internet dan komponen sistem apa pun di lingkungan data pemegang kartu.		Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
1.3	Melarang akses publik langsung antara Internet dan komponen sistem apa pun di lingkungan data pemegang kartu.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3	Melarang akses publik langsung antara Internet dan komponen sistem apa pun di lingkungan data pemegang kartu.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
1.3	Melarang akses publik langsung antara Internet dan komponen sistem apa pun di lingkungan data pemegang kartu.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3	Melarang akses publik langsung antara Internet dan komponen sistem apa pun di lingkungan data pemegang kartu.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
1.3	Melarang akses publik langsung antara Internet dan komponen sistem apa pun di lingkungan data pemegang kartu.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3	Melarang akses publik langsung antara Internet dan komponen sistem apa pun di lingkungan data pemegang kartu.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
1.3	Melarang akses publik langsung antara Internet dan komponen sistem apa pun di lingkungan data pemegang kartu.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3	Melarang akses publik langsung antara Internet dan komponen sistem apa pun di lingkungan data pemegang kartu.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3	Melarang akses publik langsung antara Internet dan komponen sistem apa pun di lingkungan data pemegang kartu.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3	Melarang akses publik langsung antara Internet dan komponen sistem apa pun di lingkungan data pemegang kartu.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3	Melarang akses publik langsung antara Internet dan komponen sistem apa pun di lingkungan data pemegang kartu.	netfw-stateless-rule-group-tidak-kosong	Grup aturan AWS Network Firewall berisi aturan yang menentukan bagaimana firewall Anda memproses lalu lintas di VPC Anda. Grup aturan stateless kosong saat ada dalam kebijakan firewall tidak memproses lalu lintas.
1.3	Melarang akses publik langsung antara Internet dan komponen sistem apa pun di lingkungan data pemegang kartu.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3	Melarang akses publik langsung antara Internet dan komponen sistem apa pun di lingkungan data pemegang kartu.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3	Melarang akses publik langsung antara Internet dan komponen sistem apa pun di lingkungan data pemegang kartu.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
1.3	Melarang akses publik langsung antara Internet dan komponen sistem apa pun di lingkungan data pemegang kartu.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3	Melarang akses publik langsung antara Internet dan komponen sistem apa pun di lingkungan data pemegang kartu.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3	Melarang akses publik langsung antara Internet dan komponen sistem apa pun di lingkungan data pemegang kartu.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3	Melarang akses publik langsung antara Internet dan komponen sistem apa pun di lingkungan data pemegang kartu.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3	Melarang akses publik langsung antara Internet dan komponen sistem apa pun di lingkungan data pemegang kartu.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
1.3	Melarang akses publik langsung antara Internet dan komponen sistem apa pun di lingkungan data pemegang kartu.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3	Melarang akses publik langsung antara Internet dan komponen sistem apa pun di lingkungan data pemegang kartu.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
1.3	Melarang akses publik langsung antara Internet dan komponen sistem apa pun di lingkungan data pemegang kartu.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3	Melarang akses publik langsung antara Internet dan komponen sistem apa pun di lingkungan data pemegang kartu.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.
1.3	Melarang akses publik langsung antara Internet dan komponen sistem apa pun di lingkungan data pemegang kartu.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3	Melarang akses publik langsung antara Internet dan komponen sistem apa pun di lingkungan data pemegang kartu.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3	Melarang akses publik langsung antara Internet dan komponen sistem apa pun di lingkungan data pemegang kartu.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.6	Tempatkan komponen sistem yang menyimpan data pemegang kartu (seperti database) di zona jaringan internal, dipisahkan dari DMZ dan jaringan tidak tepercaya lainnya.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.6	Tempatkan komponen sistem yang menyimpan data pemegang kartu (seperti database) di zona jaringan internal, dipisahkan dari DMZ dan jaringan tidak tepercaya lainnya.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
1.3.6	Tempatkan komponen sistem yang menyimpan data pemegang kartu (seperti database) di zona jaringan internal, dipisahkan dari DMZ dan jaringan tidak tepercaya lainnya.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.6	Tempatkan komponen sistem yang menyimpan data pemegang kartu (seperti database) di zona jaringan internal, dipisahkan dari DMZ dan jaringan tidak tepercaya lainnya.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
1.3.6	Tempatkan komponen sistem yang menyimpan data pemegang kartu (seperti database) di zona jaringan internal, dipisahkan dari DMZ dan jaringan tidak tepercaya lainnya.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.6	Tempatkan komponen sistem yang menyimpan data pemegang kartu (seperti database) di zona jaringan internal, dipisahkan dari DMZ dan jaringan tidak tepercaya lainnya.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.6	Tempatkan komponen sistem yang menyimpan data pemegang kartu (seperti database) di zona jaringan internal, dipisahkan dari DMZ dan jaringan tidak tepercaya lainnya.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.6	Tempatkan komponen sistem yang menyimpan data pemegang kartu (seperti database) di zona jaringan internal, dipisahkan dari DMZ dan jaringan tidak tepercaya lainnya.	netfw-policy-rule-group-terkait	Kebijakan AWS Network Firewall mendefinisikan bagaimana firewall Anda memantau dan menangani lalu lintas di VPC Amazon. Anda mengonfigurasi grup aturan stateless dan stateful untuk memfilter paket dan arus lalu lintas, dan Anda menentuka n penanganan lalu lintas default.
1.3.6	Tempatkan komponen sistem yang menyimpan data pemegang kartu (seperti database) di zona jaringan internal, dipisahkan dari DMZ dan jaringan tidak tepercaya lainnya.	netfw-stateless-rule-group-tidak-kosong	Grup aturan AWS Network Firewall berisi aturan yang menentukan bagaimana firewall Anda memproses lalu lintas di VPC Anda. Grup aturan stateless kosong saat ada dalam kebijakan firewall tidak memproses lalu lintas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.6	Tempatkan komponen sistem yang menyimpan data pemegang kartu (seperti database) di zona jaringan internal, dipisahkan dari DMZ dan jaringan tidak tepercaya lainnya.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.6	Tempatkan komponen sistem yang menyimpan data pemegang kartu (seperti database) di zona jaringan internal, dipisahkan dari DMZ dan jaringan tidak tepercaya lainnya.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
1.3.6	Tempatkan komponen sistem yang menyimpan data pemegang kartu (seperti database) di zona jaringan internal, dipisahkan dari DMZ dan jaringan tidak tepercaya lainnya.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.6	Tempatkan komponen sistem yang menyimpan data pemegang kartu (seperti database) di zona jaringan internal, dipisahkan dari DMZ dan jaringan tidak tepercaya lainnya.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.6	Tempatkan komponen sistem yang menyimpan data pemegang kartu (seperti database) di zona jaringan internal, dipisahkan dari DMZ dan jaringan tidak tepercaya lainnya.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.6	Tempatkan komponen sistem yang menyimpan data pemegang kartu (seperti database) di zona jaringan internal, dipisahkan dari DMZ dan jaringan tidak tepercaya lainnya.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.6	Tempatkan komponen sistem yang menyimpan data pemegang kartu (seperti database) di zona jaringan internal, dipisahkan dari DMZ dan jaringan tidak tepercaya lainnya.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
1.3.6	Tempatkan komponen sistem yang menyimpan data pemegang kartu (seperti database) di zona jaringan internal, dipisahkan dari DMZ dan jaringan tidak tepercaya lainnya.	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.6	Tempatkan komponen sistem yang menyimpan data pemegang kartu (seperti database) di zona jaringan internal, dipisahkan dari DMZ dan jaringan tidak tepercaya lainnya.	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
1.3.6	Tempatkan komponen sistem yang menyimpan data pemegang kartu (seperti database) di zona jaringan internal, dipisahkan dari DMZ dan jaringan tidak tepercaya lainnya.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.6	Tempatkan komponen sistem yang menyimpan data pemegang kartu (seperti database) di zona jaringan internal, dipisahkan dari DMZ dan jaringan tidak tepercaya lainnya.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.6	Tempatkan komponen sistem yang menyimpan data pemegang kartu (seperti database) di zona jaringan internal, dipisahkan dari DMZ dan jaringan tidak tepercaya lainnya.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.6	Tempatkan komponen sistem yang menyimpan data pemegang kartu (seperti database) di zona jaringan internal, dipisahkan dari DMZ dan jaringan tidak tepercaya lainnya.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.1	Selalu ubah default yang disediakan vendor dan hapus atau nonaktifkan akun default yang tidak perlu sebelum menginstal sistem di jaringan. Ini berlaku untuk SEMUA kata sandi default, termasuk namun tidak terbatas pada yang digunakan oleh sistem operasi, perangkat lunak yang menyediakan layanan keamanan, akun aplikasi dan sistem, terminal point-of-sale (POS), aplikasi pembayaran, string komunitas Simple Network Management Protocol (SNMP), dll.).	rds-cluster-default-admin-periksa	Karena nama pengguna default adalah pengetahu an publik, mengubah nama pengguna default dapat membantu mengurangi permukaan serangan untuk kluster database Amazon Relational Database Service (Amazon RDS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.1	Selalu ubah default yang disediakan vendor dan hapus atau nonaktifkan akun default yang tidak perlu sebelum menginstal sistem di jaringan. Ini berlaku untuk SEMUA kata sandi default, termasuk namun tidak terbatas pada yang digunakan oleh sistem operasi, perangkat lunak yang menyediakan layanan keamanan, akun aplikasi dan sistem, terminal point-of-sale (POS), aplikasi pembayaran, string komunitas Simple Network Management Protocol (SNMP), dll.).	rds-instance-default-admin-periksa	Karena nama pengguna default adalah pengetahu an publik, mengubah nama pengguna default dapat membantu mengurangi permukaan serangan untuk instans database Amazon Relational Database Service (Amazon RDS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.1	Selalu ubah default yang disediakan vendor dan hapus atau nonaktifkan akun default yang tidak perlu sebelum menginstal sistem di jaringan. Ini berlaku untuk SEMUA kata sandi default, termasuk namun tidak terbatas pada yang digunakan oleh sistem operasi, perangkat lunak yang menyediakan layanan keamanan, akun aplikasi dan sistem, terminal point-of-sale (POS), aplikasi pembayaran, string komunitas Simple Network Management Protocol (SNMP), dll.).	redshift-default-admin-check	Karena nama pengguna default adalah pengetahuan publik, mengubah nama pengguna default dapat membantu mengurangi permukaan serangan untuk klaster Amazon Redshift Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.1	Selalu ubah default yang disediakan vendor dan hapus atau nonaktifkan akun default yang tidak perlu sebelum menginstal sistem di jaringan. Ini berlaku untuk SEMUA kata sandi default, termasuk namun tidak terbatas pada yang digunakan oleh sistem operasi, perangkat lunak yang menyediakan layanan keamanan, akun aplikasi dan sistem, terminal point-of-sale (POS), aplikasi pembayaran, string komunitas Simple Network Management Protocol (SNMP), dll.).	redshift-default-db-name-periksa	Nama default adalah pengetahuan publik dan harus diubah pada konfigurasi. Mengubah nama database default cluster Amazon Redshift Anda dapat membantu mengurangi permukaan serangan untuk cluster Redshift Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.1	Selalu ubah default yang disediakan vendor dan hapus atau nonaktifkan akun default yang tidak perlu sebelum menginstal sistem di jaringan. Ini berlaku untuk SEMUA kata sandi default, termasuk namun tidak terbatas pada yang digunakan oleh sistem operasi, perangkat lunak yang menyediakan layanan keamanan, akun aplikasi dan sistem, terminal point-of-sale (POS), aplikasi pembayaran, string komunitas Simple Network Management Protocol (SNMP), dll.).	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.1	Selalu ubah default yang disediakan vendor dan hapus atau nonaktifkan akun default yang tidak perlu sebelum menginstal sistem di jaringan. Ini berlaku untuk SEMUA kata sandi default, termasuk namun tidak terbatas pada yang digunakan oleh sistem operasi, perangkat lunak yang menyediakan layanan keamanan, akun aplikasi dan sistem, terminal point-of-sale (POS), aplikasi pembayaran, string komunitas Simple Network Management Protocol (SNMP), dll.).	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	access-keys-rotated	Kredensi diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastika n kunci akses IAM diputar sebagaima na ditentukan oleh kebijakan organisas i. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurang i dampak bisnis jika kunci dikompromikan. Aturan ini memerluka n nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	account-part-of-or ganizations	Manajemen terpusat Akun AWS dalam AWS Organizations membantu memastika n bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabkan konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	autoscaling-launch -config-public-ip- dinonaktifkan	Jika Anda mengonfig urasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrai l jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteks i aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	cmk-backing-key-ro tation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	ec2- instance-multiple-eni-check	Aturan ini memeriksa apakah instans Amazon Elastic Compute Cloud (Amazon EC2) Anda memiliki beberapa. ENIs Memiliki beberapa ENIs dapat menyebabkan instance dual-homed, yang berarti instance yang memiliki beberapa subnet. Ini dapat menambah kompleksitas keamanan jaringan dan memperken alkan jalur dan akses jaringan yang tidak diinginkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasa n sistem yang diterima industri. Sumber standar pengerasan sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: 'Ä¢ Center for Internet Security (CIS) ,Ä¢ Organisas i Internasional untuk Standardisasi (ISO) ,Ä¢ SysAdmin Audit Network Security (SANS) Institute ,Ä¢ National Institute of Standards Technolog y (NIST).	ec2- -periksa managedinstance-as sociation-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventari s platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	ec2- -periksa managedinstance-pa tch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	ec2- security-group-attached-to -eni-peri odik	Aturan ini memastika n grup keamanan dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) atau ke ENI. Aturan ini membantu memantau kelompok keamanan yang tidak digunakan dalam inventaris dan pengelolaan lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigurasi untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentanan keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasan sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasional untuk Standardisasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	iam-user-no-policies-periksa	Aturan ini memastika n kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapka n hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	iam-user-unused-cr edentials-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharus kan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan tambahan di atas nama pengguna dan kata sandi. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	root-account-hardw are-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindun gan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	root-account-mfa-e nabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindun gan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	s3- account-level-publ ic-access -blok-per iodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediak an metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinc i untuk permintaa n yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasa n sistem yang diterima industri. Sumber standar pengerasan sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: 'Ä¢ Center for Internet Security (CIS) ,Ä¢ Organisas i Internasional untuk Standardisasi (ISO) ,Ä¢ SysAdmin Audit Network Security (SANS) Institute ,Ä¢ National Institute of Standards Technolog y (NIST).	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	s3- bucket-ssl-request s-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2	Mengembangkan standar konfigura si untuk semua komponen sistem. Pastikan bahwa standar ini mengatasi semua kerentana n keamanan yang diketahui dan konsisten dengan standar pengerasan sistem yang diterima industri. Sumber standar pengerasa n sistem yang diterima industri dapat mencakup, tetapi tidak terbatas pada: • Pusat Keamanan Internet (CIS) • Organisasi Internasi onal untuk Standardi sasi (ISO) • Institut Keamanan Jaringan SysAdmin Audit (SANS) • Institut Teknologi Standar Nasional (NIST).	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.2	Aktifkan hanya layanan, protokol, daemon, dll yang diperluka n, sebagaimana diperlukan untuk fungsi sistem.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.2	Aktifkan hanya layanan, protokol, daemon, dll yang diperluka n, sebagaimana diperlukan untuk fungsi sistem.	autoscaling-launch -config-public-ip-dinonaktifkan	Jika Anda mengonfig urasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
2.2.2	Aktifkan hanya layanan, protokol, daemon, dll yang diperluka n, sebagaimana diperlukan untuk fungsi sistem.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.2	Aktifkan hanya layanan, protokol, daemon, dll yang diperluka n, sebagaimana diperlukan untuk fungsi sistem.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
2.2.2	Aktifkan hanya layanan, protokol, daemon, dll yang diperluka n, sebagaimana diperlukan untuk fungsi sistem.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.2	Aktifkan hanya layanan, protokol, daemon, dll yang diperluka n, sebagaimana diperlukan untuk fungsi sistem.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.2	Aktifkan hanya layanan, protokol, daemon, dll yang diperluka n, sebagaimana diperlukan untuk fungsi sistem.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.2	Aktifkan hanya layanan, protokol, daemon, dll yang diperluka n, sebagaimana diperlukan untuk fungsi sistem.	lambda-function-pu blic-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotens i menyebabkan degradasi ketersedi aan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.2	Aktifkan hanya layanan, protokol, daemon, dll yang diperluka n, sebagaimana diperlukan untuk fungsi sistem.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.2	Aktifkan hanya layanan, protokol, daemon, dll yang diperluka n, sebagaimana diperlukan untuk fungsi sistem.	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
2.2.2	Aktifkan hanya layanan, protokol, daemon, dll yang diperluka n, sebagaimana diperlukan untuk fungsi sistem.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.2	Aktifkan hanya layanan, protokol, daemon, dll yang diperluka n, sebagaimana diperlukan untuk fungsi sistem.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
2.2.2	Aktifkan hanya layanan, protokol, daemon, dll yang diperluka n, sebagaimana diperlukan untuk fungsi sistem.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.2	Aktifkan hanya layanan, protokol, daemon, dll yang diperluka n, sebagaimana diperlukan untuk fungsi sistem.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.2	Aktifkan hanya layanan, protokol, daemon, dll yang diperluka n, sebagaimana diperlukan untuk fungsi sistem.	s3- account-level-publ ic-access -blok-per iodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPubl icAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.2	Aktifkan hanya layanan, protokol, daemon, dll yang diperluka n, sebagaimana diperlukan untuk fungsi sistem.	s3- -dilarang bucket-le vel-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
2.2.2	Aktifkan hanya layanan, protokol, daemon, dll yang diperluka n, sebagaimana diperlukan untuk fungsi sistem.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.2	Aktifkan hanya layanan, protokol, daemon, dll yang diperluka n, sebagaimana diperlukan untuk fungsi sistem.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
2.2.2	Aktifkan hanya layanan, protokol, daemon, dll yang diperluka n, sebagaimana diperlukan untuk fungsi sistem.	sagemaker-notebook -no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.2	Aktifkan hanya layanan, protokol, daemon, dll yang diperluka n, sebagaimana diperlukan untuk fungsi sistem.	ssm-document-not-p ublic	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkin kan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspo s informasi tentang akun, sumber daya, dan proses internal Anda.
2.2.2	Aktifkan hanya layanan, protokol, daemon, dll yang diperluka n, sebagaimana diperlukan untuk fungsi sistem.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurk an ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.2	Aktifkan hanya layanan, protokol, daemon, dll yang diperluka n, sebagaimana diperlukan untuk fungsi sistem.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.2	Aktifkan hanya layanan, protokol, daemon, dll yang diperluka n, sebagaimana diperlukan untuk fungsi sistem.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/ 0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.3	Menerapkan fitur keamanan tambahan untuk setiap layanan, protokol, atau daemon yang diperlukan yang dianggap tidak aman.	alb-desync-mode-check	Untuk membantu melindungi aplikasi untuk kerentanan HTTP Desync, pastikan mode mitigasi HTTP Desync diaktifkan pada penyeimbang beban aplikasi Anda. Masalah HTTP Desync dapat menyebabkan penyelundupan permintaan dan membuat aplikasi Anda rentan terhadap antrian permintaan atau keracunan cache. Mode mitigasi desync adalah monitor, defensif, dan paling ketat. Defensif adalah mode default.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.3	Enkripsi semua akses administratif non-konsol menggunakan kriptografi yang kuat.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
2.3	Enkripsi semua akses administratif non-konsol menggunakan kriptografi yang kuat.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.3	Enkripsi semua akses administratif non-konsol menggunakan kriptografi yang kuat.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
2.3	Enkripsi semua akses administratif non-konsol menggunakan kriptografi yang kuat.	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
2.3	Enkripsi semua akses administratif non-konsol menggunakan kriptografi yang kuat.	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.4	Pertahankan inventaris komponen sistem yang berada dalam lingkup PCI DSS.	ec2- security-group-attached-to -eni-periodik	Aturan ini memastikan grup keamanan dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) atau ke ENI. Aturan ini membantu memantau kelompok keamanan yang tidak digunakan dalam inventaris dan pengelolaan lingkungan Anda.
2.4	Pertahankan inventaris komponen sistem yang berada dalam lingkup PCI DSS.	terlampir eip	Aturan ini memastikan Elastic IPs dialokasikan ke Amazon Virtual Private Cloud (Amazon VPC) dilampirkan ke instans Amazon Elastic Compute Cloud (EC2Amazon) atau Antarmuka Jaringan Elastis yang sedang digunakan. Aturan ini membantu memantau yang tidak digunakan EIPs di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.4	Pertahankan inventaris komponen sistem yang berada dalam lingkup PCI DSS.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.4	Pertahankan inventaris komponen sistem yang berada dalam lingkup PCI DSS.	vpc-network-acl-unused-periksa	Aturan ini memastikan bahwa daftar kontrol akses jaringan Amazon Virtual Private Cloud (VPC) sedang digunakan. Pemantauan untuk daftar kontrol akses jaringan yang tidak digunakan dapat membantu inventaris dan pengelolaan lingkungan Anda yang akurat.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1	Menjaga penyimpan an data pemegang kartu seminimal mungkin dengan menerapkan kebijakan penyimpan an dan pembuanga n data, prosedur, dan proses yang mencakup setidakny a hal-hal berikut untuk semua penyimpanan data pemegang kartu (PJK): • Membatasi jumlah penyimpan an data dan waktu penyimpanan untuk yang diperlukan untuk persyaratan hukum, peraturan, dan/atau bisnis • Persyaratan penyimpanan khusus untuk data pemegang kartu • Proses penghapusan data secara aman saat tidak lagi diperluka n • Proses triwulana n untuk mengident ifikasi dan menghapus pemegang kartu yang disimpan secara aman data yang	s3- lifecycle-policy-c heck	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihk an objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	melebihi retensi yang ditentukan.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1	Menjaga penyimpanan data pemegang kartu seminimal mungkin dengan menerapkan kebijakan penyimpanan dan pembuangan data, prosedur, dan proses yang mencakup setidaknya hal-hal berikut untuk semua penyimpanan data pemegang kartu (PJK): • Membatasi jumlah penyimpanan data dan waktu penyimpanan untuk yang diperlukan untuk persyaratan hukum, peraturan, dan/atau bisnis • Persyaratan penyimpanan khusus untuk data pemegang kartu • Proses penghapusan data secara aman saat tidak lagi diperlukan • Proses triwulanan untuk mengidentifikasi dan menghapus pemegang kartu yang disimpan secara aman data yang	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup Anda diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	melebihi retensi yang ditentukan.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1	Menjaga penyimpanan data pemegang kartu seminimal mungkin dengan menerapkan kebijakan penyimpanan dan pembuangan data, prosedur, dan proses yang mencakup setidaknya hal-hal berikut untuk semua penyimpanan data pemegang kartu (PJK): • Membatasi jumlah penyimpanan data dan waktu penyimpanan untuk yang diperlukan untuk persyaratan hukum, peraturan, dan/atau bisnis • Persyaratan penyimpanan khusus untuk data pemegang kartu • Proses penghapusan data secara aman saat tidak lagi diperlukan • Proses triwulanan untuk mengidentifikasi dan menghapus pemegang kartu yang disimpan secara aman data yang	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	melebihi retensi yang ditentukan.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1	Menjaga penyimpan an data pemegang kartu seminimal mungkin dengan menerapkan kebijakan penyimpan an dan pembuanga n data, prosedur, dan proses yang mencakup setidakny a hal-hal berikut untuk semua penyimpanan data pemegang kartu (PJK): • Membatasi jumlah penyimpan an data dan waktu penyimpanan untuk yang diperlukan untuk persyaratan hukum, peraturan, dan/atau bisnis • Persyaratan penyimpanan khusus untuk data pemegang kartu • Proses penghapusan data secara aman saat tidak lagi diperluka n • Proses triwulana n untuk mengident ifikasi dan menghapus pemegang kartu yang disimpan secara aman data yang	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	melebihi retensi yang ditentukan.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4	Render PAN tidak dapat dibaca di mana pun disimpan (termasuk pada media digital portabel, media cadangan, dan dalam log) dengan menggunakan salah satu pendekata n berikut: • Hash satu arah berdasark an kriptografi yang kuat, (hash harus dari seluruh PAN) • Pemotongan (hashing tidak dapat digunakan untuk menggantikan segmen PAN yang terpotong) • Token dan bantalan indeks (bantalan harus disimpan dengan aman) • Kriptografi yang kuat dengan proses manajemen kunci terkait dan prosedur. Catatan: Ini adalah upaya yang relatif sepele bagi individu jahat untuk merekonstruksi data PAN asli jika mereka memiliki akses ke versi PAN yang	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	terpotong dan di-hash. Jika versi yang di-hash dan terpotong dari PAN yang sama ada di lingkunga n entitas, kontrol tambahan harus ada untuk memastikan bahwa versi hash dan terpotong tidak dapat dikorelasikan untuk merekonstruksi PAN asli.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4	Render PAN tidak dapat dibaca di mana pun disimpan (termasuk pada media digital portabel, media cadangan, dan dalam log) dengan menggunakan salah satu pendekata n berikut: • Hash satu arah berdasark an kriptografi yang kuat, (hash harus dari seluruh PAN) • Pemotongan (hashing tidak dapat digunakan untuk menggantikan segmen PAN yang terpotong) • Token dan bantalan indeks (bantalan harus disimpan dengan aman) • Kriptografi yang kuat dengan proses manajemen kunci terkait dan prosedur. Catatan: Ini adalah upaya yang relatif sepele bagi individu jahat untuk merekonstruksi data PAN asli jika mereka memiliki akses ke versi PAN yang	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrai l jejak Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	terpotong dan di-hash. Jika versi yang di-hash dan terpotong dari PAN yang sama ada di lingkunga n entitas, kontrol tambahan harus ada untuk memastikan bahwa versi hash dan terpotong tidak dapat dikorelasikan untuk merekonstruksi PAN asli.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4	Render PAN tidak dapat dibaca di mana pun disimpan (termasuk pada media digital portabel, media cadangan, dan dalam log) dengan menggunakan salah satu pendekata n berikut: • Hash satu arah berdasark an kriptografi yang kuat, (hash harus dari seluruh PAN) • Pemotongan (hashing tidak dapat digunakan untuk menggantikan segmen PAN yang terpotong) • Token dan bantalan indeks (bantalan harus disimpan dengan aman) • Kriptografi yang kuat dengan proses manajemen kunci terkait dan prosedur. Catatan: Ini adalah upaya yang relatif sepele bagi individu jahat untuk merekonstruksi data PAN asli jika mereka memiliki akses ke versi PAN yang	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat , pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	terpotong dan di-hash. Jika versi yang di-hash dan terpotong dari PAN yang sama ada di lingkunga n entitas, kontrol tambahan harus ada untuk memastikan bahwa versi hash dan terpotong tidak dapat dikorelasikan untuk merekonstruksi PAN asli.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4	Render PAN tidak dapat dibaca di mana pun disimpan (termasuk pada media digital portabel, media cadangan, dan dalam log) dengan menggunakan salah satu pendekata n berikut: • Hash satu arah berdasark an kriptografi yang kuat, (hash harus dari seluruh PAN) • Pemotongan (hashing tidak dapat digunakan untuk menggantikan segmen PAN yang terpotong) • Token dan bantalan indeks (bantalan harus disimpan dengan aman) • Kriptografi yang kuat dengan proses manajemen kunci terkait dan prosedur. Catatan: Ini adalah upaya yang relatif sepele bagi individu jahat untuk merekonstruksi data PAN asli jika mereka memiliki akses ke versi PAN yang	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	terpotong dan di-hash. Jika versi yang di-hash dan terpotong dari PAN yang sama ada di lingkunga n entitas, kontrol tambahan harus ada untuk memastikan bahwa versi hash dan terpotong tidak dapat dikorelasikan untuk merekonstruksi PAN asli.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4	Render PAN tidak dapat dibaca di mana pun disimpan (termasuk pada media digital portabel, media cadangan, dan dalam log) dengan menggunakan salah satu pendekata n berikut: • Hash satu arah berdasark an kriptografi yang kuat, (hash harus dari seluruh PAN) • Pemotongan (hashing tidak dapat digunakan untuk menggantikan segmen PAN yang terpotong) • Token dan bantalan indeks (bantalan harus disimpan dengan aman) • Kriptografi yang kuat dengan proses manajemen kunci terkait dan prosedur. Catatan: Ini adalah upaya yang relatif sepele bagi individu jahat untuk merekonstruksi data PAN asli jika mereka memiliki akses ke versi PAN yang	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	terpotong dan di-hash. Jika versi yang di-hash dan terpotong dari PAN yang sama ada di lingkunga n entitas, kontrol tambahan harus ada untuk memastikan bahwa versi hash dan terpotong tidak dapat dikorelasikan untuk merekonstruksi PAN asli.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4	Render PAN tidak dapat dibaca di mana pun disimpan (termasuk pada media digital portabel, media cadangan, dan dalam log) dengan menggunakan salah satu pendekata n berikut: • Hash satu arah berdasark an kriptografi yang kuat, (hash harus dari seluruh PAN) • Pemotongan (hashing tidak dapat digunakan untuk menggantikan segmen PAN yang terpotong) • Token dan bantalan indeks (bantalan harus disimpan dengan aman) • Kriptografi yang kuat dengan proses manajemen kunci terkait dan prosedur. Catatan: Ini adalah upaya yang relatif sepele bagi individu jahat untuk merekonstruksi data PAN asli jika mereka memiliki akses ke versi PAN yang	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindung i data saat istirahat , pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	terpotong dan di-hash. Jika versi yang di-hash dan terpotong dari PAN yang sama ada di lingkunga n entitas, kontrol tambahan harus ada untuk memastikan bahwa versi hash dan terpotong tidak dapat dikorelasikan untuk merekonstruksi PAN asli.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4	Render PAN tidak dapat dibaca di mana pun disimpan (termasuk pada media digital portabel, media cadangan, dan dalam log) dengan menggunakan salah satu pendekata n berikut: • Hash satu arah berdasark an kriptografi yang kuat, (hash harus dari seluruh PAN) • Pemotongan (hashing tidak dapat digunakan untuk menggantikan segmen PAN yang terpotong) • Token dan bantalan indeks (bantalan harus disimpan dengan aman) • Kriptografi yang kuat dengan proses manajemen kunci terkait dan prosedur. Catatan: Ini adalah upaya yang relatif sepele bagi individu jahat untuk merekonstruksi data PAN asli jika mereka memiliki akses ke versi PAN yang	rds-snapshot-encry pted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat , aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	terpotong dan di-hash. Jika versi yang di-hash dan terpotong dari PAN yang sama ada di lingkunga n entitas, kontrol tambahan harus ada untuk memastikan bahwa versi hash dan terpotong tidak dapat dikorelasikan untuk merekonstruksi PAN asli.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4	Render PAN tidak dapat dibaca di mana pun disimpan (termasuk pada media digital portabel, media cadangan, dan dalam log) dengan menggunakan salah satu pendekata n berikut: • Hash satu arah berdasark an kriptografi yang kuat, (hash harus dari seluruh PAN) • Pemotongan (hashing tidak dapat digunakan untuk menggantikan segmen PAN yang terpotong) • Token dan bantalan indeks (bantalan harus disimpan dengan aman) • Kriptografi yang kuat dengan proses manajemen kunci terkait dan prosedur. Catatan: Ini adalah upaya yang relatif sepele bagi individu jahat untuk merekonstruksi data PAN asli jika mereka memiliki akses ke versi PAN yang	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	terpotong dan di-hash. Jika versi yang di-hash dan terpotong dari PAN yang sama ada di lingkunga n entitas, kontrol tambahan harus ada untuk memastikan bahwa versi hash dan terpotong tidak dapat dikorelasikan untuk merekonstruksi PAN asli.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4	Render PAN tidak dapat dibaca di mana pun disimpan (termasuk pada media digital portabel, media cadangan, dan dalam log) dengan menggunakan salah satu pendekata n berikut: • Hash satu arah berdasark an kriptografi yang kuat, (hash harus dari seluruh PAN) • Pemotongan (hashing tidak dapat digunakan untuk menggantikan segmen PAN yang terpotong) • Token dan bantalan indeks (bantalan harus disimpan dengan aman) • Kriptografi yang kuat dengan proses manajemen kunci terkait dan prosedur. Catatan: Ini adalah upaya yang relatif sepele bagi individu jahat untuk merekonstruksi data PAN asli jika mereka memiliki akses ke versi PAN yang	redshift-cluster-c onfiguration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastika n bahwa konfigura si yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberika n informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapka n untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	terpotong dan di-hash. Jika versi yang di-hash dan terpotong dari PAN yang sama ada di lingkunga n entitas, kontrol tambahan harus ada untuk memastikan bahwa versi hash dan terpotong tidak dapat dikorelasikan untuk merekonstruksi PAN asli.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4	Render PAN tidak dapat dibaca di mana pun disimpan (termasuk pada media digital portabel, media cadangan, dan dalam log) dengan menggunakan salah satu pendekata n berikut: • Hash satu arah berdasark an kriptografi yang kuat, (hash harus dari seluruh PAN) • Pemotongan (hashing tidak dapat digunakan untuk menggantikan segmen PAN yang terpotong) • Token dan bantalan indeks (bantalan harus disimpan dengan aman) • Kriptografi yang kuat dengan proses manajemen kunci terkait dan prosedur. Catatan: Ini adalah upaya yang relatif sepele bagi individu jahat untuk merekonstruksi data PAN asli jika mereka memiliki akses ke versi PAN yang	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	terpotong dan di-hash. Jika versi yang di-hash dan terpotong dari PAN yang sama ada di lingkunga n entitas, kontrol tambahan harus ada untuk memastikan bahwa versi hash dan terpotong tidak dapat dikorelasikan untuk merekonstruksi PAN asli.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4	Render PAN tidak dapat dibaca di mana pun disimpan (termasuk pada media digital portabel, media cadangan, dan dalam log) dengan menggunakan salah satu pendekata n berikut: • Hash satu arah berdasark an kriptografi yang kuat, (hash harus dari seluruh PAN) • Pemotongan (hashing tidak dapat digunakan untuk menggantikan segmen PAN yang terpotong) • Token dan bantalan indeks (bantalan harus disimpan dengan aman) • Kriptografi yang kuat dengan proses manajemen kunci terkait dan prosedur. Catatan: Ini adalah upaya yang relatif sepele bagi individu jahat untuk merekonstruksi data PAN asli jika mereka memiliki akses ke versi PAN yang	s3- default-encryption -kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	terpotong dan di-hash. Jika versi yang di-hash dan terpotong dari PAN yang sama ada di lingkunga n entitas, kontrol tambahan harus ada untuk memastikan bahwa versi hash dan terpotong tidak dapat dikorelasikan untuk merekonstruksi PAN asli.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4	Render PAN tidak dapat dibaca di mana pun disimpan (termasuk pada media digital portabel, media cadangan, dan dalam log) dengan menggunakan salah satu pendekata n berikut: • Hash satu arah berdasark an kriptografi yang kuat, (hash harus dari seluruh PAN) • Pemotongan (hashing tidak dapat digunakan untuk menggantikan segmen PAN yang terpotong) • Token dan bantalan indeks (bantalan harus disimpan dengan aman) • Kriptografi yang kuat dengan proses manajemen kunci terkait dan prosedur. Catatan: Ini adalah upaya yang relatif sepele bagi individu jahat untuk merekonstruksi data PAN asli jika mereka memiliki akses ke versi PAN yang	sagemaker-endpoint -configuration-kms- kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	terpotong dan di-hash. Jika versi yang di-hash dan terpotong dari PAN yang sama ada di lingkunga n entitas, kontrol tambahan harus ada untuk memastikan bahwa versi hash dan terpotong tidak dapat dikorelasikan untuk merekonstruksi PAN asli.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4	Render PAN tidak dapat dibaca di mana pun disimpan (termasuk pada media digital portabel, media cadangan, dan dalam log) dengan menggunakan salah satu pendekata n berikut: • Hash satu arah berdasark an kriptografi yang kuat, (hash harus dari seluruh PAN) • Pemotongan (hashing tidak dapat digunakan untuk menggantikan segmen PAN yang terpotong) • Token dan bantalan indeks (bantalan harus disimpan dengan aman) • Kriptografi yang kuat dengan proses manajemen kunci terkait dan prosedur. Catatan: Ini adalah upaya yang relatif sepele bagi individu jahat untuk merekonstruksi data PAN asli jika mereka memiliki akses ke versi PAN yang	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	terpotong dan di-hash. Jika versi yang di-hash dan terpotong dari PAN yang sama ada di lingkunga n entitas, kontrol tambahan harus ada untuk memastikan bahwa versi hash dan terpotong tidak dapat dikorelasikan untuk merekonstruksi PAN asli.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.4	Render PAN tidak dapat dibaca di mana pun disimpan (termasuk pada media digital portabel, media cadangan, dan dalam log) dengan menggunakan salah satu pendekata n berikut: • Hash satu arah berdasark an kriptografi yang kuat, (hash harus dari seluruh PAN) • Pemotongan (hashing tidak dapat digunakan untuk menggantikan segmen PAN yang terpotong) • Token dan bantalan indeks (bantalan harus disimpan dengan aman) • Kriptografi yang kuat dengan proses manajemen kunci terkait dan prosedur. Catatan: Ini adalah upaya yang relatif sepele bagi individu jahat untuk merekonstruksi data PAN asli jika mereka memiliki akses ke versi PAN yang	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	terpotong dan di-hash. Jika versi yang di-hash dan terpotong dari PAN yang sama ada di lingkunga n entitas, kontrol tambahan harus ada untuk memastikan bahwa versi hash dan terpotong tidak dapat dikorelasikan untuk merekonstruksi PAN asli.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.2	Batasi akses ke kunci kriptografi ke jumlah penjaga paling sedikit yang diperlukan.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.2	Batasi akses ke kunci kriptografi ke jumlah penjaga paling sedikit yang diperlukan.	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.3	Simpan kunci rahasia dan pribadi yang digunakan untuk mengenkripsi/mendekripsi data pemegang kartu dalam satu (atau lebih) formulir berikut setiap saat: • Dienkripsi dengan kunci enkripsi kunci yang setidaknya sekuat kunci enkripsi data, dan itu disimpan secara terpisah dari kunci enkripsi data • Dalam perangkat kriptografi yang aman (seperti modul keamanan perangkat keras (host) (HSM) atau PTS-Perangkat yang disetujui point-of-interaction) • Sebagai setidaknya dua komponen kunci penuh atau saham utama, sesuai dengan metode yang diterima industri Catatan: Tidak diperlukan bahwa kunci publik disimpan di salah satu bentuk-bentuk ini.	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.3	Simpan kunci rahasia dan pribadi yang digunakan untuk mengenkripsi/mendekripsi data pemegang kartu dalam satu (atau lebih) formulir berikut setiap saat: • Dienkripsi dengan kunci enkripsi kunci yang setidaknya sekuat kunci enkripsi data, dan itu disimpan secara terpisah dari kunci enkripsi data • Dalam perangkat kriptografi yang aman (seperti modul keamanan perangkat keras (host) (HSM) atau PTS-Perangkat yang disetujui point-of-interaction) • Sebagai setidaknya dua komponen kunci penuh atau saham utama, sesuai dengan metode yang diterima industri Catatan: Tidak diperlukan bahwa kunci publik disimpan di salah satu bentuk-bentuk ini.	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.3	Simpan kunci rahasia dan pribadi yang digunakan untuk mengenkripsi/mendekripsi data pemegang kartu dalam satu (atau lebih) formulir berikut setiap saat: • Dienkripsi dengan kunci enkripsi kunci yang setidaknya sekuat kunci enkripsi data, dan itu disimpan secara terpisah dari kunci enkripsi data • Dalam perangkat kriptografi yang aman (seperti modul keamanan perangkat keras (host) (HSM) atau PTS-Perangkat yang disetujui point-of-interaction) • Sebagai setidaknya dua komponen kunci penuh atau saham utama, sesuai dengan metode yang diterima industri Catatan: Tidak diperlukan bahwa kunci publik disimpan di salah satu bentuk-bentuk ini.	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.4	Perubahan kunci kriptografi untuk kunci yang telah mencapai akhir kriptoperiode mereka (misalnya , setelah periode waktu tertentu telah berlalu dan/atau setelah sejumlah teks sandi diproduksi oleh kunci tertentu), sebagaimana didefinisikan oleh vendor aplikasi terkait atau pemilik kunci, dan berdasarkan praktik dan pedoman terbaik industri (misalnya , Publikasi Khusus NIST 800-57).	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.5	Pensiun atau penggantian (misalnya, pengarsipan, penghancuran, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised. Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification tujuan.	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.7	Pencegahan substitusi kunci kriptografi yang tidak sah.	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Gunakan protokol kriptografi dan keamanan yang kuat untuk melindung i data pemegang kartu sensitif selama transmisi melalui jaringan publik yang terbuka, termasuk yang berikut: • Hanya kunci dan sertifikat tepercaya yang diterima. • Protokol yang digunakan hanya mendukung versi atau konfigurasi yang aman. • Kekuatan enkripsi sesuai untuk metodologi enkripsi yang digunakan. Contoh jaringan publik terbuka termasuk tetapi tidak terbatas pada: • Internet • Teknologi nirkabel, termasuk 802.11 dan Bluetooth • Teknologi seluler, misalnya, Sistem Global untuk komunikasi Seluler (GSM), akses ganda divisi kode (CDMA) • Layanan Radio Paket	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastika n sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExp iration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Umum (GPRS) • Komunikasi satelit		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Gunakan protokol kriptografi dan keamanan yang kuat untuk melindung i data pemegang kartu sensitif selama transmisi melalui jaringan publik yang terbuka, termasuk yang berikut: • Hanya kunci dan sertifikat tepercaya yang diterima. • Protokol yang digunakan hanya mendukung versi atau konfigurasi yang aman. • Kekuatan enkripsi sesuai untuk metodologi enkripsi yang digunakan. Contoh jaringan publik terbuka termasuk tetapi tidak terbatas pada: • Internet • Teknologi nirkabel, termasuk 802.11 dan Bluetooth • Teknologi seluler, misalnya, Sistem Global untuk komunikasi Seluler (GSM), akses ganda divisi kode (CDMA) • Layanan Radio Paket	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Umum (GPRS) • Komunikasi satelit		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Gunakan protokol kriptografi dan keamanan yang kuat untuk melindung i data pemegang kartu sensitif selama transmisi melalui jaringan publik yang terbuka, termasuk yang berikut: • Hanya kunci dan sertifikat tepercaya yang diterima. • Protokol yang digunakan hanya mendukung versi atau konfigurasi yang aman. • Kekuatan enkripsi sesuai untuk metodologi enkripsi yang digunakan. Contoh jaringan publik terbuka termasuk tetapi tidak terbatas pada: • Internet • Teknologi nirkabel, termasuk 802.11 dan Bluetooth • Teknologi seluler, misalnya, Sistem Global untuk komunikasi Seluler (GSM), akses ganda divisi kode (CDMA) • Layanan Radio Paket	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Umum (GPRS) • Komunikasi satelit		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Gunakan protokol kriptografi dan keamanan yang kuat untuk melindung i data pemegang kartu sensitif selama transmisi melalui jaringan publik yang terbuka, termasuk yang berikut: • Hanya kunci dan sertifikat tepercaya yang diterima. • Protokol yang digunakan hanya mendukung versi atau konfigurasi yang aman. • Kekuatan enkripsi sesuai untuk metodologi enkripsi yang digunakan. Contoh jaringan publik terbuka termasuk tetapi tidak terbatas pada: • Internet • Teknologi nirkabel, termasuk 802.11 dan Bluetooth • Teknologi seluler, misalnya, Sistem Global untuk komunikasi Seluler (GSM), akses ganda divisi kode (CDMA) • Layanan Radio Paket	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-n ode enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkrip si memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Umum (GPRS) • Komunikasi satelit		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Gunakan protokol kriptografi dan keamanan yang kuat untuk melindung i data pemegang kartu sensitif selama transmisi melalui jaringan publik yang terbuka, termasuk yang berikut: • Hanya kunci dan sertifikat tepercaya yang diterima. • Protokol yang digunakan hanya mendukung versi atau konfigurasi yang aman. • Kekuatan enkripsi sesuai untuk metodologi enkripsi yang digunakan. Contoh jaringan publik terbuka termasuk tetapi tidak terbatas pada: • Internet • Teknologi nirkabel, termasuk 802.11 dan Bluetooth • Teknologi seluler, misalnya, Sistem Global untuk komunikasi Seluler (GSM), akses ganda divisi kode (CDMA) • Layanan Radio Paket	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Umum (GPRS) • Komunikasi satelit		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Gunakan protokol kriptografi dan keamanan yang kuat untuk melindung i data pemegang kartu sensitif selama transmisi melalui jaringan publik yang terbuka, termasuk yang berikut: • Hanya kunci dan sertifikat tepercaya yang diterima. • Protokol yang digunakan hanya mendukung versi atau konfigurasi yang aman. • Kekuatan enkripsi sesuai untuk metodologi enkripsi yang digunakan. Contoh jaringan publik terbuka termasuk tetapi tidak terbatas pada: • Internet • Teknologi nirkabel, termasuk 802.11 dan Bluetooth • Teknologi seluler, misalnya, Sistem Global untuk komunikasi Seluler (GSM), akses ganda divisi kode (CDMA) • Layanan Radio Paket	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Umum (GPRS) • Komunikasi satelit		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Gunakan protokol kriptografi dan keamanan yang kuat untuk melindung i data pemegang kartu sensitif selama transmisi melalui jaringan publik yang terbuka, termasuk yang berikut: • Hanya kunci dan sertifikat tepercaya yang diterima. • Protokol yang digunakan hanya mendukung versi atau konfigurasi yang aman. • Kekuatan enkripsi sesuai untuk metodologi enkripsi yang digunakan. Contoh jaringan publik terbuka termasuk tetapi tidak terbatas pada: • Internet • Teknologi nirkabel, termasuk 802.11 dan Bluetooth • Teknologi seluler, misalnya, Sistem Global untuk komunikasi Seluler (GSM), akses ganda divisi kode (CDMA) • Layanan Radio Paket	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindung i data dalam perjalana n, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Umum (GPRS) • Komunikasi satelit		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Gunakan protokol kriptografi dan keamanan yang kuat untuk melindung i data pemegang kartu sensitif selama transmisi melalui jaringan publik yang terbuka, termasuk yang berikut: • Hanya kunci dan sertifikat tepercaya yang diterima. • Protokol yang digunakan hanya mendukung versi atau konfigurasi yang aman. • Kekuatan enkripsi sesuai untuk metodologi enkripsi yang digunakan. Contoh jaringan publik terbuka termasuk tetapi tidak terbatas pada: • Internet • Teknologi nirkabel, termasuk 802.11 dan Bluetooth • Teknologi seluler, misalnya, Sistem Global untuk komunikasi Seluler (GSM), akses ganda divisi kode (CDMA) • Layanan Radio Paket	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-n ode enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkrip si memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Umum (GPRS) • Komunikasi satelit		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Gunakan protokol kriptografi dan keamanan yang kuat untuk melindung i data pemegang kartu sensitif selama transmisi melalui jaringan publik yang terbuka, termasuk yang berikut: • Hanya kunci dan sertifikat tepercaya yang diterima. • Protokol yang digunakan hanya mendukung versi atau konfigurasi yang aman. • Kekuatan enkripsi sesuai untuk metodologi enkripsi yang digunakan. Contoh jaringan publik terbuka termasuk tetapi tidak terbatas pada: • Internet • Teknologi nirkabel, termasuk 802.11 dan Bluetooth • Teknologi seluler, misalnya, Sistem Global untuk komunikasi Seluler (GSM), akses ganda divisi kode (CDMA) • Layanan Radio Paket	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Umum (GPRS) • Komunikasi satelit		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.1	Gunakan protokol kriptografi dan keamanan yang kuat untuk melindung i data pemegang kartu sensitif selama transmisi melalui jaringan publik yang terbuka, termasuk yang berikut: • Hanya kunci dan sertifikat tepercaya yang diterima. • Protokol yang digunakan hanya mendukung versi atau konfigurasi yang aman. • Kekuatan enkripsi sesuai untuk metodologi enkripsi yang digunakan. Contoh jaringan publik terbuka termasuk tetapi tidak terbatas pada: • Internet • Teknologi nirkabel, termasuk 802.11 dan Bluetooth • Teknologi seluler, misalnya, Sistem Global untuk komunikasi Seluler (GSM), akses ganda divisi kode (CDMA) • Layanan Radio Paket	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	Umum (GPRS) • Komunikasi satelit		
6.2	Pastikan bahwa semua komponen sistem dan perangkat lunak dilindungi dari kerentanan yang diketahui dengan menginstal patch keamanan yang disediakan vendor yang berlaku. Instal patch keamanan kritis dalam waktu satu bulan setelah rilis. Catatan: Patch keamanan kritis harus diidentifikasi sesuai dengan proses peringkat risiko yang ditentukan dalam Persyaratan 6.1.	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.2	Pastikan bahwa semua komponen sistem dan perangkat lunak dilindungi dari kerentanan yang diketahui dengan menginstal patch keamanan yang disediakan vendor yang berlaku. Instal patch keamanan kritis dalam waktu satu bulan setelah rilis. Catatan: Patch keamanan kritis harus diidentifikasi sesuai dengan proses peringkat risiko yang ditentukan dalam Persyaratan 6.1.	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.2	Pastikan bahwa semua komponen sistem dan perangkat lunak dilindungi dari kerentanan yang diketahui dengan menginstal patch keamanan yang disediakan vendor yang berlaku. Instal patch keamanan kritis dalam waktu satu bulan setelah rilis. Catatan: Patch keamanan kritis harus diidentifikasi sesuai dengan proses peringkat risiko yang ditentukan dalam Persyaratan 6.1.	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.2	Pastikan bahwa semua komponen sistem dan perangkat lunak dilindungi dari kerentanan yang diketahui dengan menginstal patch keamanan yang disediakan vendor yang berlaku. Instal patch keamanan kritis dalam waktu satu bulan setelah rilis. Catatan: Patch keamanan kritis harus diidentifikasi sesuai dengan proses peringkat risiko yang ditentukan dalam Persyaratan 6.1.	ecs-fargate-latest-platform-versi	Pembaruan dan tambalan keamanan diterapkan secara otomatis untuk tugas Fargate AWS Anda. Jika ditemukan masalah keamanan yang memengaru hi versi platform AWS Fargate, AWS tambal versi platform. Untuk membantu pengelolaan tambalan tugas Amazon Elastic Container Service (ECS) yang menjalank an AWS Fargate, perbarui tugas mandiri layanan Anda untuk menggunakan versi platform terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.2	Pastikan bahwa semua komponen sistem dan perangkat lunak dilindungi dari kerentanan yang diketahui dengan menginstal patch keamanan yang disediakan vendor yang berlaku. Instal patch keamanan kritis dalam waktu satu bulan setelah rilis. Catatan: Patch keamanan kritis harus diidentifikasi sesuai dengan proses peringkat risiko yang ditentukan dalam Persyaratan 6.1.	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relational Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.2	Pastikan bahwa semua komponen sistem dan perangkat lunak dilindungi dari kerentanan yang diketahui dengan menginstal patch keamanan yang disediakan vendor yang berlaku. Instal patch keamanan kritis dalam waktu satu bulan setelah rilis. Catatan: Patch keamanan kritis harus diidentifikasi sesuai dengan proses peringkat risiko yang ditentukan dalam Persyaratan 6.1.	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.3.2	Tinjau kode khusus sebelum dirilis ke produksi atau pelanggan untuk mengidentifikasi potensi kerentana n pengkodean (menggunakan proses manual atau otomatis) untuk memasukka n setidaknya hal-hal berikut: • Perubahan kode ditinjau oleh individu selain penulis kode asal, dan oleh individu yang memiliki pengetahuan tentang teknik peninjauan kode dan praktik pengkodean yang aman. • Tinjauan kode memastika n kode dikembang kan sesuai dengan pedoman pengkodean yang aman • Koreksi yang tepat diterapka n sebelum rilis. • Hasil tinjauan kode ditinjau dan disetujui oleh manajemen sebelum rilis. (Lanjutan di halaman berikutnya)	ecr-private-image-scanning-diaktifkan	Pemindaian gambar Amazon Elastic Container Repositor y (ECR) membantu mengidentifikasi kerentanan perangkat lunak dalam gambar kontainer Anda. Mengaktifkan pemindaian gambar pada repositori ECR menambahk an lapisan verifikasi untuk integritas dan keamanan gambar yang disimpan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.6	Untuk aplikasi web yang dihadapi publik, atasi ancaman dan kerentanan baru secara berkelanj utan dan pastikan aplikasi ini dilindung i dari serangan yang diketahui dengan salah satu metode berikut: • Meninjau aplikasi web yang menghadap publik dari alat atau metode penilaian keamanan kerentanan aplikasi manual atau otomatis, setidaknya setiap tahun dan setelah perubahan apa pun Catatan: Penilaian ini tidak sama dengan pemindaian kerentana n yang dilakukan untuk Persyaratan 11.2. Menginstal solusi teknis otomatis yang mendeteks i dan mencegah serangan berbasis web (misalnya, firewall aplikasi web) di depan aplikasi web yang menghadap	alb-desync-mode-ch eck	Untuk membantu melindungi aplikasi untuk kerentana n HTTP Desync, pastikan mode mitigasi HTTP Desync diaktifkan pada penyeimba ng beban aplikasi Anda. Masalah HTTP Desync dapat menyebabk an penyelundupan permintaan dan membuat aplikasi Anda rentan terhadap antrian permintaa n atau keracunan cache. Mode mitigasi desync adalah monitor, defensif, dan paling ketat. Defensif adalah mode default.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	publik, untuk terus memeriksa semua lalu lintas.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.6	Untuk aplikasi web yang dihadapi publik, atasi ancaman dan kerentanan baru secara berkelanj utan dan pastikan aplikasi ini dilindung i dari serangan yang diketahui dengan salah satu metode berikut: • Meninjau aplikasi web yang menghadap publik dari alat atau metode penilaian keamanan kerentanan aplikasi manual atau otomatis, setidaknya setiap tahun dan setelah perubahan apa pun Catatan: Penilaian ini tidak sama dengan pemindaian kerentana n yang dilakukan untuk Persyaratan 11.2. Menginstal solusi teknis otomatis yang mendeteks i dan mencegah serangan berbasis web (misalnya, firewall aplikasi web) di depan aplikasi web yang menghadap	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	publik, untuk terus memeriksa semua lalu lintas.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.6	Untuk aplikasi web yang dihadapi publik, atasi ancaman dan kerentanan baru secara berkelanj utan dan pastikan aplikasi ini dilindung i dari serangan yang diketahui dengan salah satu metode berikut: • Meninjau aplikasi web yang menghadap publik dari alat atau metode penilaian keamanan kerentanan aplikasi manual atau otomatis, setidaknya setiap tahun dan setelah perubahan apa pun Catatan: Penilaian ini tidak sama dengan pemindaian kerentana n yang dilakukan untuk Persyaratan 11.2. Menginstal solusi teknis otomatis yang mendeteks i dan mencegah serangan berbasis web (misalnya, firewall aplikasi web) di depan aplikasi web yang menghadap	api-gw-associated-with-waf	AWS WAF memungkinkan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizink an, memblokir, atau menghitung permintaa n web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindung inya dari serangan berbahaya

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	publik, untuk terus memeriksa semua lalu lintas.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.6	Untuk aplikasi web yang dihadapi publik, atasi ancaman dan kerentanan baru secara berkelanj utan dan pastikan aplikasi ini dilindung i dari serangan yang diketahui dengan salah satu metode berikut: • Meninjau aplikasi web yang menghadap publik dari alat atau metode penilaian keamanan kerentanan aplikasi manual atau otomatis, setidaknya setiap tahun dan setelah perubahan apa pun Catatan: Penilaian ini tidak sama dengan pemindaian kerentana n yang dilakukan untuk Persyaratan 11.2. Menginstal solusi teknis otomatis yang mendeteks i dan mencegah serangan berbasis web (misalnya, firewall aplikasi web) di depan aplikasi web yang menghadap	waf-regional-rule-not-kosong	Pastikan AWS WAF Anda memiliki aturan yang tidak kosong. Aturan tanpa kondisi dapat mengakibatkan perilaku yang tidak diinginkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	publik, untuk terus memeriksa semua lalu lintas.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.6	Untuk aplikasi web yang dihadapi publik, atasi ancaman dan kerentanan baru secara berkelanj utan dan pastikan aplikasi ini dilindung i dari serangan yang diketahui dengan salah satu metode berikut: • Meninjau aplikasi web yang menghadap publik dari alat atau metode penilaian keamanan kerentanan aplikasi manual atau otomatis, setidaknya setiap tahun dan setelah perubahan apa pun Catatan: Penilaian ini tidak sama dengan pemindaian kerentana n yang dilakukan untuk Persyaratan 11.2. Menginstal solusi teknis otomatis yang mendeteks i dan mencegah serangan berbasis web (misalnya, firewall aplikasi web) di depan aplikasi web yang menghadap	waf-regional-rulegroup-not-kosong	Pastikan AWS WAF Anda memiliki grup aturan yang tidak kosong. Grup aturan yang kosong dapat mengakibatkan perilaku yang tidak diinginkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	publik, untuk terus memeriksa semua lalu lintas.		

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.6	Untuk aplikasi web yang dihadapi publik, atasi ancaman dan kerentanan baru secara berkelanj utan dan pastikan aplikasi ini dilindung i dari serangan yang diketahui dengan salah satu metode berikut: • Meninjau aplikasi web yang menghadap publik dari alat atau metode penilaian keamanan kerentanan aplikasi manual atau otomatis, setidaknya setiap tahun dan setelah perubahan apa pun Catatan: Penilaian ini tidak sama dengan pemindaian kerentana n yang dilakukan untuk Persyaratan 11.2. Menginstal solusi teknis otomatis yang mendeteks i dan mencegah serangan berbasis web (misalnya, firewall aplikasi web) di depan aplikasi web yang menghadap	waf-regional-webacl-not-kosong	Web ACL yang dilampirkan ke AWS WAF dapat berisi kumpulan aturan dan kelompok aturan untuk memeriksa dan mengontrol permintaan web. Jika ACL Web kosong, lalu lintas web lewat tanpa terdeteksi atau ditindaklanjuti oleh WAF.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
	publik, untuk terus memeriksa semua lalu lintas.		
7.1.1	Tentukan kebutuhan akses untuk setiap peran, termasuk: • Komponen sistem dan sumber daya data yang setiap peran perlu akses untuk fungsi pekerjaan mereka • Tingkat hak istimewa yang diperlukan (misalnya , pengguna, administr ator, dll.) untuk mengakses sumber daya.	ecs-task-definition-nonroot-pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan bahwa pengguna non-root ditunjuk untuk mengakses definisi tugas Amazon Elastic Container Service (Amazon ECS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1.1	Tentukan kebutuhan akses untuk setiap peran, termasuk: • Komponen sistem dan sumber daya data yang setiap peran perlu akses untuk fungsi pekerjaan mereka • Tingkat hak istimewa yang diperlukan (misalnya , pengguna, administr ator, dll.) untuk mengakses sumber daya.	s3- bucket-acl-prohibi ted	Aturan ini memeriksa untuk melihat apakah Daftar Kontrol Akses (ACLs) digunakan untuk kontrol akses di Bucket Amazon S3. ACLs adalah mekanisme kontrol akses lama untuk bucket Amazon S3 yang AWS mendahulu i Identity and Access Management (IAM). Sebagai gantinya ACLs, ini adalah praktik terbaik untuk menggunakan kebijakan IAM atau kebijakan bucket S3 untuk mengelola akses ke bucket S3 Anda dengan lebih mudah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1.1	Tentukan kebutuhan akses untuk setiap peran, termasuk: • Komponen sistem dan sumber daya data yang setiap peran perlu akses untuk fungsi pekerjaan mereka • Tingkat hak istimewa yang diperlukan (misalnya , pengguna, administr ator, dll.) untuk mengakses sumber daya.	ecs-containers-non privileged	Untuk membantu menerapkan prinsip hak istimewa paling rendah, definisi tugas Amazon Elastic Container Service (Amazon ECS) seharusnya tidak mengaktifkan hak istimewa yang ditinggikan. Ketika parameter ini benar, wadah diberikan hak istimewa yang ditinggikan pada instance wadah host (mirip dengan pengguna root).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1.1	Tentukan kebutuhan akses untuk setiap peran, termasuk: • Komponen sistem dan sumber daya data yang setiap peran perlu akses untuk fungsi pekerjaan mereka • Tingkat hak istimewa yang diperlukan (misalnya , pengguna, administr ator, dll.) untuk mengakses sumber daya.	ecs-containers-rea donly-access	Mengaktifkan akses baca saja ke kontainer Amazon Elastic Container Service (ECS) dapat membantu mematuhi prinsip hak istimewa yang paling rendah. Opsi ini dapat mengurangi vektor serangan karena sistem file instance container tidak dapat dimodifikasi kecuali jika memiliki izin baca-tulis eksplisit.
7.1.1	Tentukan kebutuhan akses untuk setiap peran, termasuk: • Komponen sistem dan sumber daya data yang setiap peran perlu akses untuk fungsi pekerjaan mereka • Tingkat hak istimewa yang diperlukan (misalnya , pengguna, administr ator, dll.) untuk mengakses sumber daya.	efs-access-point-e nforce-root-direktori	Menegakkan direktori root untuk jalur akses Amazon Elastic File System (Amazon EFS) membantu membatasi akses data dengan memastikan bahwa pengguna jalur akses hanya dapat menjangkau file dari subdirektori yang ditentukan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1.1	Tentukan kebutuhan akses untuk setiap peran, termasuk: • Komponen sistem dan sumber daya data yang setiap peran perlu akses untuk fungsi pekerjaan mereka • Tingkat hak istimewa yang diperlukan (misalnya , pengguna, administr ator, dll.) untuk mengakses sumber daya.	efs-access-point-enforce-identitas pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan penegakan pengguna diaktifkan untuk Amazon Elastic File System (Amazon EFS) Anda. Saat diaktifkan, Amazon EFS mengganti kan pengguna dan grup klien NFS IDs dengan identitas yang dikonfigurasi pada titik akses untuk semua operasi sistem file dan hanya memberika n akses ke identitas pengguna yang diberlakukan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1.1	Tentukan kebutuhan akses untuk setiap peran, termasuk: • Komponen sistem dan sumber daya data yang setiap peran perlu akses untuk fungsi pekerjaan mereka • Tingkat hak istimewa yang diperlukan (misalnya , pengguna, administr ator, dll.) untuk mengakses sumber daya.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1.1	Tentukan kebutuhan akses untuk setiap peran, termasuk: • Komponen sistem dan sumber daya data yang setiap peran perlu akses untuk fungsi pekerjaan mereka • Tingkat hak istimewa yang diperlukan (misalnya , pengguna, administr ator, dll.) untuk mengakses sumber daya.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
7.1.1	Tentukan kebutuhan akses untuk setiap peran, termasuk: • Komponen sistem dan sumber daya data yang setiap peran perlu akses untuk fungsi pekerjaan mereka • Tingkat hak istimewa yang diperlukan (misalnya , pengguna, administr ator, dll.) untuk mengakses sumber daya.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1.1	Tentukan kebutuhan akses untuk setiap peran, termasuk: • Komponen sistem dan sumber daya data yang setiap peran perlu akses untuk fungsi pekerjaan mereka • Tingkat hak istimewa yang diperlukan (misalnya , pengguna, administr ator, dll.) untuk mengakses sumber daya.	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
7.1.1	Tentukan kebutuhan akses untuk setiap peran, termasuk: • Komponen sistem dan sumber daya data yang setiap peran perlu akses untuk fungsi pekerjaan mereka • Tingkat hak istimewa yang diperlukan (misalnya , pengguna, administr ator, dll.) untuk mengakses sumber daya.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1.1	Tentukan kebutuhan akses untuk setiap peran, termasuk: • Komponen sistem dan sumber daya data yang setiap peran perlu akses untuk fungsi pekerjaan mereka • Tingkat hak istimewa yang diperlukan (misalnya , pengguna, administr ator, dll.) untuk mengakses sumber daya.	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1.1	Tentukan kebutuhan akses untuk setiap peran, termasuk: • Komponen sistem dan sumber daya data yang setiap peran perlu akses untuk fungsi pekerjaan mereka • Tingkat hak istimewa yang diperlukan (misalnya , pengguna, administr ator, dll.) untuk mengakses sumber daya.	iam-policy-no-stat ements-with-full-a ccess	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1.1	Tentukan kebutuhan akses untuk setiap peran, termasuk: • Komponen sistem dan sumber daya data yang setiap peran perlu akses untuk fungsi pekerjaan mereka • Tingkat hak istimewa yang diperlukan (misalnya , pengguna, administr ator, dll.) untuk mengakses sumber daya.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1.1	Tentukan kebutuhan akses untuk setiap peran, termasuk: • Komponen sistem dan sumber daya data yang setiap peran perlu akses untuk fungsi pekerjaan mereka • Tingkat hak istimewa yang diperlukan (misalnya , pengguna, administr ator, dll.) untuk mengakses sumber daya.	iam-user-group-membership-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastika n pengguna adalah anggota setidaknya satu grup. Mengizink an pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1.1	Tentukan kebutuhan akses untuk setiap peran, termasuk: • Komponen sistem dan sumber daya data yang setiap peran perlu akses untuk fungsi pekerjaan mereka • Tingkat hak istimewa yang diperlukan (misalnya , pengguna, administr ator, dll.) untuk mengakses sumber daya.	iam-user-no-policies-periksa	Aturan ini memastika n kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapka n hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1.1	Tentukan kebutuhan akses untuk setiap peran, termasuk: • Komponen sistem dan sumber daya data yang setiap peran perlu akses untuk fungsi pekerjaan mereka • Tingkat hak istimewa yang diperlukan (misalnya , pengguna, administr ator, dll.) untuk mengakses sumber daya.	opensearch-access-control-enabled	Pastikan kontrol akses berbutir halus diaktifkan di domain Layanan Amazon OpenSearch Anda. Kontrol akses berbutir halus menyediakan mekanisme otorisasi yang disempurnakan untuk mencapai akses yang paling tidak memiliki hak istimewa ke domain Layanan Amazon. OpenSearc h Ini memungkin kan kontrol akses berbasis peran ke domain, serta indeks, dokumen, dan keamanan tingkat lapangan, dukungan untuk dasbor OpenSearc h Layanan multi-ten ancy, dan otentikas i dasar HTTP untuk Layanan dan Kibana. OpenSearch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1.2	Batasi akses ke pengguna istimewa untuk hak istimewa yang paling tidak diperlukan IDs untuk melakukan tanggung jawab pekerjaan.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
7.1.2	Batasi akses ke pengguna istimewa untuk hak istimewa yang paling tidak diperlukan IDs untuk melakukan tanggung jawab pekerjaan.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1.2	Batasi akses ke pengguna istimewa untuk hak istimewa yang paling tidak diperlukan IDs untuk melakukan tanggung jawab pekerjaan.	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi, pengembal ian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatt erns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
7.1.2	Batasi akses ke pengguna istimewa untuk hak istimewa yang paling tidak diperlukan IDs untuk melakukan tanggung jawab pekerjaan.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1.2	Batasi akses ke pengguna istimewa untuk hak istimewa yang paling tidak diperlukan IDs untuk melakukan tanggung jawab pekerjaan.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1.2	Batasi akses ke pengguna istimewa untuk hak istimewa yang paling tidak diperlukan IDs untuk melakukan tanggung jawab pekerjaan.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
7.1.2	Batasi akses ke pengguna istimewa untuk hak istimewa yang paling tidak diperlukan IDs untuk melakukan tanggung jawab pekerjaan.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1.2	Batasi akses ke pengguna istimewa untuk hak istimewa yang paling tidak diperlukan IDs untuk melakukan tanggung jawab pekerjaan.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.1.2	Batasi akses ke pengguna istimewa untuk hak istimewa yang paling tidak diperlukan IDs untuk melakukan tanggung jawab pekerjaan.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.1	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Cakupan semua komponen sistem	ecs-containers-non privileged	Untuk membantu menerapkan prinsip hak istimewa paling rendah, definisi tugas Amazon Elastic Container Service (Amazon ECS) seharusnya tidak mengaktifkan hak istimewa yang ditinggikan. Ketika parameter ini benar, wadah diberikan hak istimewa yang ditinggikan pada instance wadah host (mirip dengan pengguna root).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.1	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Cakupan semua komponen sistem	ecs-containers-readonly-access	Mengaktifkan akses baca saja ke kontainer Amazon Elastic Container Service (ECS) dapat membantu mematuhi prinsip hak istimewa yang paling rendah. Opsi ini dapat mengurangi vektor serangan karena sistem file instance container tidak dapat dimodifikasi kecuali jika memiliki izin baca-tulis eksplisit.
7.2.1	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Cakupan semua komponen sistem	efs-access-point-enforce-root-direktori	Menegakkan direktori root untuk jalur akses Amazon Elastic File System (Amazon EFS) membantu membatasi akses data dengan memastikan bahwa pengguna jalur akses hanya dapat menjangkau file dari subdirektori yang ditentukan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.1	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Cakupan semua komponen sistem	efs-access-point-enforce-identitas pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan penegakan pengguna diaktifkan untuk Amazon Elastic File System (Amazon EFS) Anda. Saat diaktifkan, Amazon EFS menggantikan pengguna dan grup klien NFS IDs dengan identitas yang dikonfigurasi pada titik akses untuk semua operasi sistem file dan hanya memberikan akses ke identitas pengguna yang diberlakukan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.1	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Cakupan semua komponen sistem	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktifkan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediakan sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.1	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Cakupan semua komponen sistem	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
7.2.1	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Cakupan semua komponen sistem	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.1	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Cakupan semua komponen sistem	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi, pengembalian, dan pendelegasian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
7.2.1	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Cakupan semua komponen sistem	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.1	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Cakupan semua komponen sistem	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.1	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Cakupan semua komponen sistem	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.1	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Cakupan semua komponen sistem	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.1	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Cakupan semua komponen sistem	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.1	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Cakupan semua komponen sistem	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.1	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Cakupan semua komponen sistem	opensearch-access-control-enabled	Pastikan kontrol akses berbutir halus diaktifkan di domain Layanan Amazon OpenSearch Anda. Kontrol akses berbutir halus menyediakan mekanisme otorisasi yang disempurnakan untuk mencapai akses yang paling tidak memiliki hak istimewa ke domain Layanan Amazon. OpenSearch Ini memungkinkan kontrol akses berbasis peran ke domain, serta indeks, dokumen, dan keamanan tingkat lapangan, dukungan untuk dasbor OpenSearch Layanan multi-tenancy, dan otentikasi dasar HTTP untuk Layanan dan Kibana. OpenSearch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.2	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Penugasan hak istimewa kepada individu berdasarkan klasifikasi dan fungsi pekerjaan.	ecs-containers-non privileged	Untuk membantu menerapkan prinsip hak istimewa paling rendah, definisi tugas Amazon Elastic Container Service (Amazon ECS) seharusnya tidak mengaktifkan hak istimewa yang ditinggikan. Ketika parameter ini benar, wadah diberikan hak istimewa yang ditinggikan pada instance wadah host (mirip dengan pengguna root).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.2	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Penugasan hak istimewa kepada individu berdasarkan klasifikasi dan fungsi pekerjaan.	ecs-containers-readonly-access	Mengaktifkan akses baca saja ke kontainer Amazon Elastic Container Service (ECS) dapat membantu mematuhi prinsip hak istimewa yang paling rendah. Opsi ini dapat mengurangi vektor serangan karena sistem file instance container tidak dapat dimodifikasi kecuali jika memiliki izin baca-tulis eksplisit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.2	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Penugasan hak istimewa kepada individu berdasarkan klasifikasi dan fungsi pekerjaan.	efs-access-point-enforce-root-direktori	Menegakkan direktori root untuk jalur akses Amazon Elastic File System (Amazon EFS) membantu membatasi akses data dengan memastikan bahwa pengguna jalur akses hanya dapat menjangkau file dari subdirektori yang ditentukan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.2	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Penugasan hak istimewa kepada individu berdasarkan klasifikasi dan fungsi pekerjaan.	efs-access-point-enforce-identitas pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan penegakan pengguna diaktifkan untuk Amazon Elastic File System (Amazon EFS) Anda. Saat diaktifkan, Amazon EFS mengganti kan pengguna dan grup klien NFS IDs dengan identitas yang dikonfigurasi pada titik akses untuk semua operasi sistem file dan hanya memberika n akses ke identitas pengguna yang diberlakukan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.2	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Penugasan hak istimewa kepada individu berdasarkan klasifikasi dan fungsi pekerjaan.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktifkan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengautentikasi dikenal sebagai prinsipal. Prinsipal ada dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediakan sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluarkan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.2	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Penugasan hak istimewa kepada individu berdasarkan klasifikasi dan fungsi pekerjaan.	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda
7.2.2	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Penugasan hak istimewa kepada individu berdasarkan klasifikasi dan fungsi pekerjaan.	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.2	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Penugasan hak istimewa kepada individu berdasarkan klasifikasi dan fungsi pekerjaan.	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizinkan tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi, pengembalian, dan pendelegasian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncrypt From Nilai aktual

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			harus mencerminkan kebijakan organisasi Anda.
7.2.2	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Penugasan hak istimewa kepada individu berdasarkan klasifikasi dan fungsi pekerjaan.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.2	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Penugasan hak istimewa kepada individu berdasarkan klasifikasi dan fungsi pekerjaan.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.2	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Penugasan hak istimewa kepada individu berdasarkan klasifikasi dan fungsi pekerjaan.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.2	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Penugasan hak istimewa kepada individu berdasarkan klasifikasi dan fungsi pekerjaan.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.2	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Penugasan hak istimewa kepada individu berdasarkan klasifikasi dan fungsi pekerjaan.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.2	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Penugasan hak istimewa kepada individu berdasarkan klasifikasi dan fungsi pekerjaan.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.2	Menetapkan sistem kontrol akses untuk komponen sistem yang membatasi akses berdasarkan kebutuhan pengguna untuk mengetahui, dan diatur untuk “menolak semua” kecuali secara khusus diizinkan. Sistem kontrol akses ini harus mencakup yang berikut: Penugasan hak istimewa kepada individu berdasarkan klasifikasi dan fungsi pekerjaan.	opensearch-access-control-enabled	Pastikan kontrol akses berbutir halus diaktifkan di domain Layanan Amazon OpenSearch Anda. Kontrol akses berbutir halus menyediakan mekanisme otorisasi yang disempurnakan untuk mencapai akses yang paling tidak memiliki hak istimewa ke domain Layanan Amazon. OpenSearch Ini memungkinkan kontrol akses berbasis peran ke domain, serta indeks, dokumen, dan keamanan tingkat lapangan, dukungan untuk dasbor OpenSearch Layanan multi-tenancy, dan otentikasi dasar HTTP untuk Layanan dan Kibana. OpenSearch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.3	Pengaturan “deny-all” default.	s3- bucket-acl-prohibited	Aturan ini memeriksa untuk melihat apakah Daftar Kontrol Akses (ACLs) digunakan untuk kontrol akses di Bucket Amazon S3. ACLs adalah mekanisme kontrol akses lama untuk bucket Amazon S3 yang AWS mendahului Identity and Access Management (IAM). Sebagai gantinya ACLs, ini adalah praktik terbaik untuk menggunakan kebijakan IAM atau kebijakan bucket S3 untuk mengelola akses ke bucket S3 Anda dengan lebih mudah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.1.1	Tetapkan semua pengguna ID unik sebelum mengizinkan mereka mengakses komponen sistem atau data pemegang kartu.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.1.4	Hapus/nonaktifkan akun pengguna yang tidak aktif dalam waktu 90 hari.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsageUsia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.1	Menggunakan kriptografi yang kuat, membuat semua kredensi otentikasi (seperti kata sandi/frasa) tidak dapat dibaca selama transmisi dan penyimpanan pada semua komponen sistem.	codebuild-project-environment-privileged-periksa	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan lingkungan CodeBuild proyek Amazon Anda tidak mengaktifkan mode istimewa. Pengaturan ini harus dinonaktifkan untuk mencegah akses yang tidak diinginkan ke Docker APIs serta perangkat keras yang mendasarinya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.1	Menggunakan kriptografi yang kuat, membuat semua kredensi otentikasi (seperti kata sandi/frasa) tidak dapat dibaca selama transmisi dan penyimpanan pada semua komponen sistem.	ecs-no-environment-secrets	Sebagai praktik terbaik keamanan, berikan informasi sensitif ke wadah sebagai variabel lingkungan. Anda dapat menyuntikkan data dengan aman ke dalam wadah Amazon Elastic Container Service (ECS) dengan mereferensikan nilai yang disimpan di AWS Systems Manager Parameter Store atau AWS Secrets Manager dalam definisi container definisi tugas Amazon ECS. Kemudian, Anda dapat mengekspos informasi sensitif Anda sebagai variabel lingkungan atau dalam konfigurasi log wadah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.1	Menggunakan kriptografi yang kuat, membuat semua kredensi otentikasi (seperti kata sandi/frasa) tidak dapat dibaca selama transmisi dan penyimpanan pada semua komponen sistem.	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
8.2.1	Menggunakan kriptografi yang kuat, membuat semua kredensi otentikasi (seperti kata sandi/frasa) tidak dapat dibaca selama transmisi dan penyimpanan pada semua komponen sistem.	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengautentikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.1	Menggunakan kriptografi yang kuat, membuat semua kredensi otentikasi (seperti kata sandi/frasa) tidak dapat dibaca selama transmisi dan penyimpanan pada semua komponen sistem.	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
8.2.1	Menggunakan kriptografi yang kuat, membuat semua kredensi otentikasi (seperti kata sandi/frasa) tidak dapat dibaca selama transmisi dan penyimpanan pada semua komponen sistem.	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.1	Menggunakan kriptografi yang kuat, membuat semua kredensi otentikasi (seperti kata sandi/frasa) tidak dapat dibaca selama transmisi dan penyimpanan pada semua komponen sistem.	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
8.2.1	Menggunakan kriptografi yang kuat, membuat semua kredensi otentikasi (seperti kata sandi/frasa) tidak dapat dibaca selama transmisi dan penyimpanan pada semua komponen sistem.	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
8.2.1	Menggunakan kriptografi yang kuat, membuat semua kredensi otentikasi (seperti kata sandi/frasa) tidak dapat dibaca selama transmisi dan penyimpanan pada semua komponen sistem.	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.1	Menggunakan kriptografi yang kuat, membuat semua kredensi otentikasi (seperti kata sandi/frasa) tidak dapat dibaca selama transmisi dan penyimpanan pada semua komponen sistem.	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
8.2.1	Menggunakan kriptografi yang kuat, membuat semua kredensi otentikasi (seperti kata sandi/frasa) tidak dapat dibaca selama transmisi dan penyimpanan pada semua komponen sistem.	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.1	Menggunakan kriptografi yang kuat, membuat semua kredensi otentikasi (seperti kata sandi/frasa) tidak dapat dibaca selama transmisi dan penyimpanan pada semua komponen sistem.	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.1	Menggunakan kriptografi yang kuat, membuat semua kredensi otentikasi (seperti kata sandi/frasa) tidak dapat dibaca selama transmisi dan penyimpanan pada semua komponen sistem.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.1	Menggunakan kriptografi yang kuat, membuat semua kredensi otentikasi (seperti kata sandi/frasa) tidak dapat dibaca selama transmisi dan penyimpanan pada semua komponen sistem.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
8.2.1	Menggunakan kriptografi yang kuat, membuat semua kredensi otentikasi (seperti kata sandi/frasa) tidak dapat dibaca selama transmisi dan penyimpanan pada semua komponen sistem.	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.1	Menggunakan kriptografi yang kuat, membuat semua kredensi otentikasi (seperti kata sandi/frasa) tidak dapat dibaca selama transmisi dan penyimpanan pada semua komponen sistem.	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
8.2.1	Menggunakan kriptografi yang kuat, membuat semua kredensi otentikasi (seperti kata sandi/frasa) tidak dapat dibaca selama transmisi dan penyimpanan pada semua komponen sistem.	sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.1	Menggunakan kriptografi yang kuat, membuat semua kredensi otentikasi (seperti kata sandi/frasa) tidak dapat dibaca selama transmisi dan penyimpanan pada semua komponen sistem.	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
8.2.1	Menggunakan kriptografi yang kuat, membuat semua kredensi otentikasi (seperti kata sandi/frasa) tidak dapat dibaca selama transmisi dan penyimpanan pada semua komponen sistem.	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.1	Menggunakan kriptografi yang kuat, membuat semua kredensi otentikasi (seperti kata sandi/frasa) tidak dapat dibaca selama transmisi dan penyimpanan pada semua komponen sistem.	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.3	Kata sandi/frasa sandi harus memenuhi yang berikut: • Memerlukan panjang minimal tujuh karakter. • Berisi karakter numerik dan alfabet. Atau, kata sandi/frasa sandi harus memiliki kompleksitas dan kekuatan setidaknya setara dengan parameter yang ditentukan di atas.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk secara opsional mengatur RequireUppercaseCharacters (PCI DSS default: false), RequireLowercaseCharacters (PCI DSS default: true), (PCI DSS default: false), RequireSymbols (PCI DSS default: true), RequireNumbers (PCI DSS default: 7), MinimumPasswordLength (PCI

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			DSS default: 4), dan PasswordReusePrevention MaxPasswordAge (PCI DSS default: 90) untuk Kebijakan IAM Password Anda. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.4	Ubah kata sandi/frasa sandi pengguna setidaknya setelah setiap 90 hari.	access-keys-rotated	Kredensi diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.4	Ubah kata sandi/frasa sandi pengguna setidaknya setelah setiap 90 hari.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk secara opsional mengatur RequireUppercaseCharacters (PCI DSS default: false), RequireLowercaseCharacters (PCI DSS default: true), (PCI DSS default: false), RequireSymbols (PCI DSS default: true), RequireNumbers (PCI DSS default: 7), MinimumPasswordLength (PCI

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			DSS default: 4), dan PasswordReusePrevention MaxPasswordAge (PCI DSS default: 90) untuk Kebijakan IAM Password Anda. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
8.2.4	Ubah kata sandi/frasa sandi pengguna setidaknya setelah setiap 90 hari.	secretsmanager-rotation-enabled-check	Aturan ini memastikan AWS rahasia Secrets Manager telah diaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.5	Jangan biarkan seseorang mengirimkan barang baru password/passphrase that is the same as any of the last four passwords/passphrases yang telah dia gunakan.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk secara opsional mengatur RequireUppercaseCharacters (PCI DSS default: false), RequireLowercaseCharacters (PCI DSS default: true), (PCI DSS default: false), RequireSymbols (PCI DSS default: true), RequireNumbers (PCI DSS default: 7), MinimumPasswordLength (PCI

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			DSS default: 4), dan PasswordR eusePrevention MaxPasswordAge (PCI DSS default: 90) untuk Kebijakan IAM Password Anda. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
8.3.1	Menggabungkan otentikasi multi-fak tor untuk semua akses non-konsol ke dalam CDE untuk personel dengan akses administratif.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastika n otentikasi multi-fak tor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.1	Menggabungkan otentikasi multi-faktor untuk semua akses non-konsol ke dalam CDE untuk personel dengan akses administratif.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.1	Menggabungkan otentikasi multi-faktor untuk semua akses non-konsol ke dalam CDE untuk personel dengan akses administratif.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.1	Menggabungkan otentikasi multi-faktor untuk semua akses non-konsol ke dalam CDE untuk personel dengan akses administratif.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.2	Menggabungkan otentikasi multi-faktor untuk semua akses jaringan jarak jauh (baik pengguna maupun administrator, dan termasuk akses pihak ketiga untuk dukungan atau pemeliharaan) yang berasal dari luar jaringan entitas.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.2	Menggabungkan otentikasi multi-faktor untuk semua akses jaringan jarak jauh (baik pengguna maupun administrator, dan termasuk akses pihak ketiga untuk dukungan atau pemeliharaan) yang berasal dari luar jaringan entitas.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.2	Menggabungkan otentikasi multi-faktor untuk semua akses jaringan jarak jauh (baik pengguna maupun administrator, dan termasuk akses pihak ketiga untuk dukungan atau pemeliharaan) yang berasal dari luar jaringan entitas.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.2	Menggabungkan otentikasi multi-faktor untuk semua akses jaringan jarak jauh (baik pengguna maupun administrator, dan termasuk akses pihak ketiga untuk dukungan atau pemeliharaan) yang berasal dari luar jaringan entitas.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan tambahan untuk nama pengguna dan kata sandi. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
10.1	Menerapkan jejak audit untuk menghubungkan semua akses ke komponen sistem ke setiap pengguna individu.	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.1	Menerapkan jejak audit untuk menghubungkan semua akses ke komponen sistem ke setiap pengguna individu.	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifkan. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.1	Menerapkan jejak audit untuk menghubungkan semua akses ke komponen sistem ke setiap pengguna individu.	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.1	Menerapkan jejak audit untuk menghubungkan semua akses ke komponen sistem ke setiap pengguna individu.	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.1	Menerapkan jejak audit untuk menghubungkan semua akses ke komponen sistem ke setiap pengguna individu.	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.1	Menerapkan jejak audit untuk menghubungkan semua akses ke komponen sistem ke setiap pengguna individu.	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.1	Menerapkan jejak audit untuk menghubungkan semua akses ke komponen sistem ke setiap pengguna individu.	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
10.1	Menerapkan jejak audit untuk menghubungkan semua akses ke komponen sistem ke setiap pengguna individu.	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.1	Menerapkan jejak audit untuk menghubungkan semua akses ke komponen sistem ke setiap pengguna individu.	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.
10.1	Menerapkan jejak audit untuk menghubungkan semua akses ke komponen sistem ke setiap pengguna individu.	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.1	Menerapkan jejak audit untuk menghubungkan semua akses ke komponen sistem ke setiap pengguna individu.	opensearch-audit-logging-enabled	Pastikan pencatatan audit diaktifkan di domain OpenSearch Layanan Amazon Anda. Pencatatan audit memungkinkan Anda melacak aktivitas pengguna di OpenSearch domain Anda, termasuk keberhasilan dan kegagalan otentikasi, permintaan, perubahan indeks OpenSearch, dan kueri penelusuran yang masuk.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.1	Menerapkan jejak audit untuk menghubungkan semua akses ke komponen sistem ke setiap pengguna individu.	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.1	Menerapkan jejak audit untuk menghubungkan semua akses ke komponen sistem ke setiap pengguna individu.	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.1	Menerapkan jejak audit untuk menghubungkan semua akses ke komponen sistem ke setiap pengguna individu.	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Semua pengguna individu mengakses data pemegang kartu	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Semua pengguna individu mengakses data pemegang kartu	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Semua pengguna individu mengakses data pemegang kartu	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Semua pengguna individu mengakses data pemegang kartu	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
10.2.1	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Semua pengguna individu mengakses data pemegang kartu	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Semua pengguna individu mengakses data pemegang kartu	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.
10.2.1	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Semua pengguna individu mengakses data pemegang kartu	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Semua pengguna individu mengakses data pemegang kartu	opensearch-audit-logging-enabled	Pastikan pencatatan audit diaktifkan di domain OpenSearch Layanan Amazon Anda. Pencatatan audit memungkinkan Anda melacak aktivitas pengguna di OpenSearch domain Anda, termasuk keberhasilan dan kegagalan otentikasi, permintaan, perubahan indeks OpenSearch, dan kueri penelusuran yang masuk.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Semua pengguna individu mengakses data pemegang kartu	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Semua pengguna individu mengakses data pemegang kartu	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Semua pengguna individu mengakses data pemegang kartu	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.2	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Semua tindakan yang diambil oleh setiap individu dengan hak akses root atau administratif	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.2	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Semua tindakan yang diambil oleh setiap individu dengan hak akses root atau administratif	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
10.2.2	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Semua tindakan yang diambil oleh setiap individu dengan hak akses root atau administratif	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.2	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Semua tindakan yang diambil oleh setiap individu dengan hak akses root atau administratif	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.
10.2.2	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Semua tindakan yang diambil oleh setiap individu dengan hak akses root atau administratif	opensearch-audit-l ogging-enabled	Pastikan pencatata n audit diaktifkan di domain OpenSearc h Layanan Amazon Anda. Pencatatan audit memungkin kan Anda melacak aktivitas pengguna di OpenSearc h domain Anda, termasuk keberhasi lan dan kegagalan otentikasi, permintaa n, perubahan indeks OpenSearch, dan kueri penelusuran yang masuk.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.2	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Semua tindakan yang diambil oleh setiap individu dengan hak akses root atau administratif	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.2	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Semua tindakan yang diambil oleh setiap individu dengan hak akses root atau administratif	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.2	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Semua tindakan yang diambil oleh setiap individu dengan hak akses root atau administratif	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.3	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Akses ke semua jejak audit	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.3	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Akses ke semua jejak audit	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
10.2.3	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Akses ke semua jejak audit	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.3	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Akses ke semua jejak audit	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.
10.2.3	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Akses ke semua jejak audit	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.3	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Akses ke semua jejak audit	opensearch-audit-logging-enabled	Pastikan pencatatan audit diaktifkan di domain OpenSearch Layanan Amazon Anda. Pencatatan audit memungkinkan Anda melacak aktivitas pengguna di OpenSearch domain Anda, termasuk keberhasilan dan kegagalan otentikasi, permintaan, perubahan indeks OpenSearch, dan kueri penelusuran yang masuk.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.3	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Akses ke semua jejak audit	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.3	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Akses ke semua jejak audit	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.3	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Akses ke semua jejak audit	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.3	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Akses ke semua jejak audit	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.4	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Upaya akses logis tidak valid	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.4	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Upaya akses logis tidak valid	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.4	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Upaya akses logis tidak valid	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.4	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Upaya akses logis tidak valid	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
10.2.4	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Upaya akses logis tidak valid	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.4	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Upaya akses logis tidak valid	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.
10.2.4	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Upaya akses logis tidak valid	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.4	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Upaya akses logis tidak valid	opensearch-audit-logging-enabled	Pastikan pencatatan audit diaktifkan di domain OpenSearch Layanan Amazon Anda. Pencatatan audit memungkinkan Anda melacak aktivitas pengguna di OpenSearch domain Anda, termasuk keberhasilan dan kegagalan otentikasi, permintaan, perubahan indeks OpenSearch, dan kueri penelusuran yang masuk.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.4	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Upaya akses logis tidak valid	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.4	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Upaya akses logis tidak valid	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.4	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Upaya akses logis tidak valid	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.5	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Penggunaan dan perubahan mekanisme identifikasi dan otentikasi—termasuk namun tidak terbatas pada pembuatan akun baru dan peningkatan hak istimewa—dan semua perubahan, penambahan, atau penghapusan ke akun dengan hak akses root atau administratif	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD_TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.5	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Penggunaan dan perubahan mekanisme identifikasi dan otentikasi—termasuk namun tidak terbatas pada pembuatan akun baru dan peningkatan hak istimewa—dan semua perubahan, penambahan, atau penghapusan ke akun dengan hak akses root atau administratif	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.5	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Penggunaan dan perubahan mekanisme identifikasi dan otentikasi—termasuk namun tidak terbatas pada pembuatan akun baru dan peningkatan hak istimewa—dan semua perubahan, penambahan, atau penghapusan ke akun dengan hak akses root atau administratif	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.5	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Penggunaan dan perubahan mekanisme identifikasi dan otentikasi—termasuk namun tidak terbatas pada pembuatan akun baru dan peningkatan hak istimewa—dan semua perubahan, penambahan, atau penghapusan ke akun dengan hak akses root atau administratif	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.5	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Penggunaan dan perubahan mekanisme identifikasi dan otentikasi—termasuk namun tidak terbatas pada pembuatan akun baru dan peningkatan hak istimewa—dan semua perubahan, penambahan, atau penghapusan ke akun dengan hak akses root atau administratif	opensearch-audit-logging-enabled	Pastikan pencatatan audit diaktifkan di domain OpenSearch Layanan Amazon Anda. Pencatatan audit memungkinkan Anda melacak aktivitas pengguna di OpenSearch domain Anda, termasuk keberhasilan dan kegagalan otentikasi, permintaan, perubahan indeks OpenSearch, dan kueri penelusuran yang masuk.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.5	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Penggunaan dan perubahan mekanisme identifikasi dan otentikasi—termasuk namun tidak terbatas pada pembuatan akun baru dan peningkatan hak istimewa—dan semua perubahan, penambahan, atau penghapusan ke akun dengan hak akses root atau administratif	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.5	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Penggunaan dan perubahan mekanisme identifikasi dan otentikasi—termasuk namun tidak terbatas pada pembuatan akun baru dan peningkatan hak istimewa—dan semua perubahan, penambahan, atau penghapusan ke akun dengan hak akses root atau administratif	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.5	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Penggunaan dan perubahan mekanisme identifikasi dan otentikasi—termasuk namun tidak terbatas pada pembuatan akun baru dan peningkatan hak istimewa—dan semua perubahan, penambahan, atau penghapusan ke akun dengan hak akses root atau administratif	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.6	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Inisialisasi, penghentian, atau jeda log audit	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.6	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Inisialisasi, penghenti an, atau jeda log audit	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.6	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Inisialisasi, penghentian, atau jeda log audit	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
10.2.7	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Pembuatan dan penghapusan objek tingkat sistem	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.7	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Pembuatan dan penghapusan objek tingkat sistem	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.7	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Pembuatan dan penghapusan objek tingkat sistem	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.7	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Pembuatan dan penghapusan objek tingkat sistem	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.
10.2.7	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Pembuatan dan penghapusan objek tingkat sistem	opensearch-audit-l ogging-enabled	Pastikan pencatata n audit diaktifkan di domain OpenSearc h Layanan Amazon Anda. Pencatatan audit memungkin kan Anda melacak aktivitas pengguna di OpenSearc h domain Anda, termasuk keberhasi lan dan kegagalan otentikasi, permintaa n, perubahan indeks OpenSearch, dan kueri penelusuran yang masuk.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.7	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Pembuatan dan penghapusan objek tingkat sistem	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.7	Menerapkan jejak audit otomatis untuk semua komponen sistem untuk merekonstruksi peristiwa berikut: Pembuatan dan penghapusan objek tingkat sistem	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
10.3.1	Catat setidakny a entri jejak audit berikut untuk semua komponen sistem untuk setiap acara: Identifikasi pengguna	api-gw-execution-l ogging-diaktifkan	Pencatatan API Gateway menampilk an tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.1	Catat setidakny a entri jejak audit berikut untuk semua komponen sistem untuk setiap acara: Identifikasi pengguna	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.1	Catat setidakny a entri jejak audit berikut untuk semua komponen sistem untuk setiap acara: Identifikasi pengguna	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.1	Catat setidakny a entri jejak audit berikut untuk semua komponen sistem untuk setiap acara: Identifikasi pengguna	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediak an metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinc i untuk permintaa n yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.1	Catat setidakny a entri jejak audit berikut untuk semua komponen sistem untuk setiap acara: Identifikasi pengguna	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.1	Catat setidakny a entri jejak audit berikut untuk semua komponen sistem untuk setiap acara: Identifikasi pengguna	wafv2-logging-diak tifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatata n AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.1	Catat setidakny a entri jejak audit berikut untuk semua komponen sistem untuk setiap acara: Identifikasi pengguna	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
10.3.1	Catat setidakny a entri jejak audit berikut untuk semua komponen sistem untuk setiap acara: Identifikasi pengguna	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteks i aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.1	Catat setidakny a entri jejak audit berikut untuk semua komponen sistem untuk setiap acara: Identifikasi pengguna	codebuild-project-logging-enabled	Pastikan pencatata n AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatc h atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.
10.3.1	Catat setidakny a entri jejak audit berikut untuk semua komponen sistem untuk setiap acara: Identifikasi pengguna	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.1	Catat setidakny a entri jejak audit berikut untuk semua komponen sistem untuk setiap acara: Identifikasi pengguna	opensearch-audit-logging-enabled	Pastikan pencatatan audit diaktifkan di domain OpenSearch Layanan Amazon Anda. Pencatatan audit memungkinkan Anda melacak aktivitas pengguna di OpenSearch domain Anda, termasuk keberhasilan dan kegagalan otentikasi, permintaan, perubahan indeks OpenSearch, dan kueri penelusuran yang masuk.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.1	Catat setidakny a entri jejak audit berikut untuk semua komponen sistem untuk setiap acara: Identifikasi pengguna	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.1	Catat setidakny a entri jejak audit berikut untuk semua komponen sistem untuk setiap acara: Identifikasi pengguna	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.1	Catat setidakny a entri jejak audit berikut untuk semua komponen sistem untuk setiap acara: Identifikasi pengguna	redshift-cluster-c onfiguration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastika n bahwa konfigura si yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberika n informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapka n untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.5	Amankan jalur audit sehingga tidak dapat diubah.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrai l jejak Anda.
10.5	Amankan jalur audit sehingga tidak dapat diubah.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
10.5	Amankan jalur audit sehingga tidak dapat diubah.	s3- default-encryption -kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.5.2	Lindungi file jejak audit dari modifikasi yang tidak sah.	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk AWS CloudTrai l jejak Anda.
10.5.2	Lindungi file jejak audit dari modifikasi yang tidak sah.	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
10.5.2	Lindungi file jejak audit dari modifikasi yang tidak sah.	s3- default-encryption -kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.5.3	Segera mencadang kan file jejak audit ke server log terpusat atau media yang sulit untuk mengubah.	s3- lifecycle-policy-c heck	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihk an objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.5.3	Segera mencadang kan file jejak audit ke server log terpusat atau media yang sulit untuk mengubah.	backup-plan-min-fr equency-and-min-re tention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkin kan Anda untuk mengatur parameter requiredFrequencyV alue (Config default: 1), (requiredR etentionDays Config default: 35) dan (requiredFrequencyU nit Config default: days). Nilai aktual harus mencerminkan persyaratan organisas i Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.5.3	Segera mencadang kan file jejak audit ke server log terpusat atau media yang sulit untuk mengubah.	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
10.5.3	Segera mencadang kan file jejak audit ke server log terpusat atau media yang sulit untuk mengubah.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.5.5	Gunakan perangkat lunak pemantauan integritas file atau deteksi perubahan pada log untuk memastikan bahwa data log yang ada tidak dapat diubah tanpa menghasilkan peringatan (meskipun data baru yang ditambahkan tidak boleh menyebabkan peringatan).	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.5.5	Gunakan perangkat lunak pemantauan integritas file atau deteksi perubahan pada log untuk memastikan bahwa data log yang ada tidak dapat diubah tanpa menghasilkan peringatan (meskipun data baru yang ditambahkan tidak boleh menyebabkan peringatan).	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertah ankan, mengambil , dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.7	Simpan riwayat jejak audit setidaknya selama satu tahun, dengan minimal tiga bulan segera tersedia untuk analisis (misalnya, online, diarsipkan, atau dapat dipulihkan dari cadangan).	s3- lifecycle-policy-check	Pastikan kebijakan siklus hidup Amazon S3 dikonfigurasi untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek (misalnya, mengalihkan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.7	Simpan riwayat jejak audit setidaknya selama satu tahun, dengan minimal tiga bulan segera tersedia untuk analisis (misalnya, online, diarsipkan, atau dapat dipulihkan dari cadangan).	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.2.3	Lakukan pemindaian internal dan eksternal , dan pemindaia n kembali sesuai kebutuhan, setelah perubahan signifika n. Pemindaian harus dilakukan oleh personel yang berkualifikasi.	ecr-private-image-scanning-diaktifkan	Pemindaian gambar Amazon Elastic Container Repositor y (ECR) membantu mengidentifikasi kerentanan perangkat lunak dalam gambar kontainer Anda. Mengaktifkan pemindaian gambar pada repositori ECR menambahk an lapisan verifikasi untuk integritas dan keamanan gambar yang disimpan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Gunakan deteksi intrusi and/or intrusion -prevention technique s to detect and/or mencegah intrusi ke dalam jaringan. Pantau semua lalu lintas di perimeter lingkungan data pemegang kartu serta pada titik-titik kritis di lingkunga n data pemegang kartu, dan mempering atkan personel untuk dugaan kompromi. Selalu perbarui semua mesin deteksi dan pencegahan intrusi, garis dasar, dan tanda tangan.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.4	Gunakan deteksi intrusi and/or intrusion -prevention technique s to detect and/or mencegah intrusi ke dalam jaringan. Pantau semua lalu lintas di perimeter lingkungan data pemegang kartu serta pada titik-titik kritis di lingkunga n data pemegang kartu, dan mempering atkan personel untuk dugaan kompromi. Selalu perbarui semua mesin deteksi dan pencegahan intrusi, garis dasar, dan tanda tangan.	netfw-policy-rule-group-terkait	Kebijakan AWS Network Firewall mendefinisikan bagaimana firewall Anda memantau dan menangani lalu lintas di VPC Amazon. Anda mengonfigurasi grup aturan stateless dan stateful untuk memfilter paket dan arus lalu lintas, dan Anda menentuka n penanganan lalu lintas default.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.5	Menyebarkan mekanisme deteksi perubahan (misalnya , alat pemantaua n integritas file) untuk mempering atkan personel untuk modifikas i yang tidak sah (termasuk perubahan , penambahan, dan penghapusan) file sistem kritis, file konfigurasi, atau file konten; dan konfigura sikan perangkat lunak untuk melakukan perbandingan file penting setidaknya setiap minggu.	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integrita s CloudTrail log. Validasi file log membantu menentuka n apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandata nganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifik asi, menghapus atau memalsukan CloudTrail file log tanpa deteksi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.5	Menyebarkan mekanisme deteksi perubahan (misalnya , alat pemantaua n integritas file) untuk mempering atkan personel untuk modifikas i yang tidak sah (termasuk perubahan , penambahan, dan penghapusan) file sistem kritis, file konfigurasi, atau file konten; dan konfigura sikan perangkat lunak untuk melakukan perbandingan file penting setidaknya setiap minggu.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk PCI DSS 3.2.1.

Praktik Terbaik Operasional untuk PCI DSS 4.0 (Tidak termasuk jenis sumber daya global)

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini menyediakan contoh pemetaan antara Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) 4.0 (Tidak termasuk tipe sumber daya global) dan aturan Config terkelola AWS . Setiap AWS Config aturan berlaku untuk AWS sumber daya tertentu, dan berhubungan dengan satu atau lebih kontrol PCI DSS. Kontrol PCI DSS dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.2.5	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	transfer-family-server-no-ftp	Pastikan server yang dibuat dengan AWS Transfer Family tidak menggunakan FTP untuk koneksi endpoint. Aturannya adalah NON_COMPLIANT jika protokol server untuk koneksi endpoint diaktifkan FTP.
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	api-gw-endpoint-type-periksa	Pastikan Amazon API Gateway APIs adalah tipe yang ditentukan dalam parameter aturan 'endpointConfigurationType'.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			Aturan mengembalikan NON_COMPLIANT jika REST API tidak cocok dengan tipe titik akhir yang dikonfigurasi dalam parameter aturan.
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	netfw-policy-default-action-fragmen-paket	Pastikan kebijakan AWS Network Firewall dikonfigurasi dengan tindakan default stateless yang ditentukan pengguna untuk paket terfragmentasi. Aturannya adalah NON_COMPLIANT jika tindakan default stateless untuk paket terfragmentasi tidak cocok dengan tindakan default yang ditentukan pengguna.
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	eks-endpoint-no-public-akses	Pastikan titik akhir Amazon Elastic Kubernetes Service (Amazon EKS) tidak dapat diakses publik. Aturannya adalah NON_COMPLIANT jika titik akhir dapat diakses publik.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	terbatas-ssh	Catatan: Untuk aturan ini, pengidentifikasi aturan (INCOMING _SSH_DISABLED) dan nama aturan (restricted-ssh) berbeda. Pastikan bahwa lalu lintas SSH yang masuk untuk grup keamanan dapat diakses. Aturannya adalah COMPLIANT jika alamat IP dari lalu lintas SSH yang masuk dalam grup keamanan dibatasi (CIDR selain 0.0.0.0/0 atau: :/0). Jika tidak, NON_COMPLIANT.
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	appsync-associated-with-waf	Pastikan AWS AppSync APIs yang terkait dengan daftar kontrol akses AWS WAFv2 web (ACLs). Aturannya adalah NON_COMPLIANT untuk AWS AppSync API jika tidak terkait dengan ACL web.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber Bitbucket TIDAK berisi kredenal masuk atau tidak. Aturannya adalah NON_COMPLIANT jika URL berisi informasi login dan COMPLIANT jika tidak.
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancers . Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	emr-block-public-access	Pastikan akun dengan Amazon EMR telah mengaktifkan pengaturan akses publik yang diblokir. Aturannya adalah NON_COMPLIANT jika BlockPublicSecurityGroupRules salah, atau jika benar, port selain Port 22 terdaftar di. PermittedPublicSecurityGroupRuleRanges
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	nacl-no-unrestricted-ssh-rdp	Pastikan port default untuk lalu lintas masuk SSH/RDP untuk daftar kontrol akses jaringan () dibatasi. NACLs Aturannya adalah NON_COMPLIANT jika entri masuk NACL memungkinkan blok sumber TCP atau UDP CIDR untuk port 22 atau 3389.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	ec2- -semua client-vpn-not-authorize	Pastikan bahwa aturan otorisasi AWS Client VPN tidak mengotorisasi akses koneksi untuk semua klien. Aturannya adalah NON_COMPLIANT jika 'AccessAll' hadir dan disetel ke true.
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	internet-gateway-authorized-vpc-hanya	Pastikan gateway internet dilampirkan ke cloud pribadi virtual resmi (Amazon VPC). Aturannya adalah NON_COMPLIANT jika gateway internet dilampirkan ke VPC yang tidak sah.
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	s3- -blok access-point-public-access	Pastikan jalur akses Amazon S3 telah mengaktifkan pengaturan akses publik blok. Aturannya adalah NON_COMPLIANT jika pengaturan akses publik blok tidak diaktifkan untuk titik akses S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	s3- -blok account-level-public-access	Pastikan bahwa pengaturan blok akses publik yang diperlukan dikonfigurasi dari tingkat akun. Aturannya hanya NON_COMPLIANT jika bidang yang ditetapkan di bawah ini tidak cocok dengan bidang yang sesuai di item konfigurasi.
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	api-gw-endpoint-type-periksa	Pastikan Amazon API Gateway APIs adalah tipe yang ditentukan dalam parameter aturan 'endpointConfigurationType'. Aturan mengembalikan NON_COMPLIANT jika REST API tidak cocok dengan tipe titik akhir yang dikonfigurasi dalam parameter aturan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	netfw-policy-default-action-fragmen-paket	Pastikan kebijakan AWS Network Firewall dikonfigurasi dengan tindakan default stateless yang ditentukan pengguna untuk paket terfragmentasi. Aturannya adalah NON_COMPLIANT jika tindakan default stateless untuk paket terfragmentasi tidak cocok dengan tindakan default yang ditentukan pengguna.
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	redshift-enhanced-vpc-routing-diaktifkan	Pastikan bahwa klaster Amazon Redshift telah 'diaktifkan. enhancedVpcRouting Aturannya adalah NON_COMPLIANT jika 'enhanced VpcRouting' tidak diaktifkan atau jika konfigurasi. enhancedVpcRouting lapangan adalah 'palsu'.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	eks-endpoint-no-public-akses	Pastikan titik akhir Amazon Elastic Kubernetes Service (Amazon EKS) tidak dapat diakses publik. Aturannya adalah NON_COMPLIANT jika titik akhir dapat diakses publik.
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	terbatas-ssh	Catatan: Untuk aturan ini, pengidentifikasi aturan (INCOMING_SSH_DISABLED) dan nama aturan (restricted-ssh) berbeda. Pastikan bahwa lalu lintas SSH yang masuk untuk grup keamanan dapat diakses. Aturannya adalah COMPLIANT jika alamat IP dari lalu lintas SSH yang masuk dalam grup keamanan dibatasi (CIDR selain 0.0.0.0/0 atau: :/0). Jika tidak, NON_COMPLIANT.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	appsync-associated-with-waf	Pastikan AWS AppSync APIs yang terkait dengan daftar kontrol akses AWS WAFv2 web (ACLs). Aturannya adalah NON_COMPLIANT untuk AWS AppSync API jika tidak terkait dengan ACL web.
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber Bitbucket TIDAK berisi kredenal masuk atau tidak. Aturannya adalah NON_COMPLIANT jika URL berisi informasi login dan COMPLIANT jika tidak.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancers . Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	emr-block-public-access	Pastikan akun dengan Amazon EMR telah mengaktifkan pengaturan akses publik yang diblokir. Aturannya adalah NON_COMPLIANT jika BlockPublicSecurityGroupRules salah, atau jika benar, port selain Port 22 terdaftar di. PermittedPublicSecurityGroupRuleRanges
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	nacl-no-unrestricted-ssh-rdp	Pastikan port default untuk lalu lintas masuk SSH/RDP untuk daftar kontrol akses jaringan () dibatasi. NACLs Aturannya adalah NON_COMPLIANT jika entri masuk NACL memungkinkan blok sumber TCP atau UDP CIDR untuk port 22 atau 3389.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	ec2- -semua client-vpn-not-authorize	Pastikan bahwa aturan otorisasi AWS Client VPN tidak mengotorisasi akses koneksi untuk semua klien. Aturannya adalah NON_COMPLIANT jika 'AccessAll' hadir dan disetel ke true.
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	internet-gateway-authorized-vpc-hanya	Pastikan gateway internet dilampirkan ke cloud pribadi virtual resmi (Amazon VPC). Aturannya adalah NON_COMPLIANT jika gateway internet dilampirkan ke VPC yang tidak sah.
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	s3- -blok access-point-public-access	Pastikan jalur akses Amazon S3 telah mengaktifkan pengaturan akses publik blok. Aturannya adalah NON_COMPLIANT jika pengaturan akses publik blok tidak diaktifkan untuk titik akses S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	s3- -blok account-level-public-access	Pastikan bahwa pengaturan blok akses publik yang diperlukan dikonfigurasi dari tingkat akun. Aturannya hanya NON_COMPLIANT jika bidang yang ditetapkan di bawah ini tidak cocok dengan bidang yang sesuai di item konfigurasi.
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	api-gw-endpoint-type-periksa	Pastikan Amazon API Gateway APIs adalah tipe yang ditentukan dalam parameter aturan 'endpointConfigurationType'. Aturan mengembalikan NON_COMPLIANT jika REST API tidak cocok dengan tipe titik akhir yang dikonfigurasi dalam parameter aturan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	netfw-policy-default-action-fragmen-paket	Pastikan kebijakan AWS Network Firewall dikonfigurasi dengan tindakan default stateless yang ditentukan pengguna untuk paket terfragmentasi. Aturannya adalah NON_COMPLIANT jika tindakan default stateless untuk paket terfragmentasi tidak cocok dengan tindakan default yang ditentukan pengguna.
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	redshift-enhanced-vpc-routing-diaktifkan	Pastikan bahwa klaster Amazon Redshift telah 'diaktifkan. enhancedVpcRouting Aturannya adalah NON_COMPLIANT jika 'enhanced VpcRouting' tidak diaktifkan atau jika konfigurasi. enhancedVpcRouting lapangan adalah 'palsu'.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	eks-endpoint-no-public-akses	Pastikan titik akhir Amazon Elastic Kubernetes Service (Amazon EKS) tidak dapat diakses publik. Aturannya adalah NON_COMPLIANT jika titik akhir dapat diakses publik.
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	terbatas-ssh	Catatan: Untuk aturan ini, pengidentifikasi aturan (INCOMING_SSH_DISABLED) dan nama aturan (restricted-ssh) berbeda. Pastikan bahwa lalu lintas SSH yang masuk untuk grup keamanan dapat diakses. Aturannya adalah COMPLIANT jika alamat IP dari lalu lintas SSH yang masuk dalam grup keamanan dibatasi (CIDR selain 0.0.0.0/0 atau: :/0). Jika tidak, NON_COMPLIANT.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	appsync-associated-with-waf	Pastikan AWS AppSync APIs yang terkait dengan daftar kontrol akses AWS WAFv2 web (ACLs). Aturannya adalah NON_COMPLIANT untuk AWS AppSync API jika tidak terkait dengan ACL web.
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber Bitbucket TIDAK berisi kredenal masuk atau tidak. Aturannya adalah NON_COMPLIANT jika URL berisi informasi login dan COMPLIANT jika tidak.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	emr-block-public-access	Pastikan akun dengan Amazon EMR telah mengaktifkan pengaturan akses publik yang diblokir. Aturannya adalah NON_COMPLIANT jika BlockPublicSecurityGroupRules salah, atau jika benar, port selain Port 22 terdaftar di. PermittedPublicSecurityGroupRuleRanges
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	nacl-no-unrestricted-ssh-rdp	Pastikan port default untuk lalu lintas masuk SSH/RDP untuk daftar kontrol akses jaringan () dibatasi. NACLs Aturannya adalah NON_COMPLIANT jika entri masuk NACL memungkinkan blok sumber TCP atau UDP CIDR untuk port 22 atau 3389.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	ec2- -semua client-vpn-not-authorize	Pastikan bahwa aturan otorisasi AWS Client VPN tidak mengotorisasi akses koneksi untuk semua klien. Aturannya adalah NON_COMPLIANT jika 'AccessAll' hadir dan disetel ke true.
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	internet-gateway-authorized-vpc-hanya	Pastikan gateway internet dilampirkan ke cloud pribadi virtual resmi (Amazon VPC). Aturannya adalah NON_COMPLIANT jika gateway internet dilampirkan ke VPC yang tidak sah.
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	s3- -blok access-point-public-access	Pastikan jalur akses Amazon S3 telah mengaktifkan pengaturan akses publik blok. Aturannya adalah NON_COMPLIANT jika pengaturan akses publik blok tidak diaktifkan untuk titik akses S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	s3- -blok account-level-public-access	Pastikan bahwa pengaturan blok akses publik yang diperlukan dikonfigurasi dari tingkat akun. Aturannya hanya NON_COMPLIANT jika bidang yang ditetapkan di bawah ini tidak cocok dengan bidang yang sesuai di item konfigurasi.
1.4.1	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendalikan. (PCI-DSS-V4.0)	api-gw-endpoint-type-periksa	Pastikan Amazon API Gateway APIs adalah tipe yang ditentukan dalam parameter aturan 'endpointConfigurationType'. Aturan mengembalikan NON_COMPLIANT jika REST API tidak cocok dengan tipe titik akhir yang dikonfigurasi dalam parameter aturan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.1	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	redshift-enhanced-vpc-routing-diaktifkan	Pastikan bahwa klaster Amazon Redshift telah 'diaktifk an. enhancedV pcRouting Aturannya adalah NON_COMPL IANT jika 'enhanced VpcRouting' tidak diaktifkan atau jika konfigurasi. enhancedVpcRouting lapangan adalah 'palsu'.
1.4.1	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	internet-gateway-a uthorized-vpc-hanya	Pastikan gateway internet dilampirkan ke cloud pribadi virtual resmi (Amazon VPC). Aturannya adalah NON_COMPLIANT jika gateway internet dilampirkan ke VPC yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	api-gw-endpoint-type-periksa	Pastikan Amazon API Gateway APIs adalah tipe yang ditentuka n dalam parameter aturan 'endpoint ConfigurationType'. Aturan mengembal ikan NON_COMPL IANT jika REST API tidak cocok dengan tipe titik akhir yang dikonfigurasi dalam parameter aturan.
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	cloudfront-custom-ssl-certificate	Pastikan sertifikat yang terkait dengan CloudFront distribus i Amazon bukan sertifikat SSL default. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi menggunak an sertifikat SSL default.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	netfw-policy-default-action-fragmen-paket	Pastikan kebijakan AWS Network Firewall dikonfigurasi dengan tindakan default stateless yang ditentukan pengguna untuk paket terfragme ntasi. Aturannya adalah NON_COMPL IANT jika tindakan default stateless untuk paket terfragmentasi tidak cocok dengan tindakan default yang ditentukan pengguna.
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	redshift-enhanced-vpc-routing-diaktifkan	Pastikan bahwa klaster Amazon Redshift telah 'diaktifk an. enhancedV pcRouting Aturannya adalah NON_COMPL IANT jika 'enhanced VpcRouting' tidak diaktifkan atau jika konfigurasi. enhancedVpcRouting lapangan adalah 'palsu'.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	eks-endpoint-no-pu blic-akses	Pastikan titik akhir Amazon Elastic Kubernetes Service (Amazon EKS) tidak dapat diakses publik. Aturannya adalah NON_COMPLIANT jika titik akhir dapat diakses publik.
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	terbatas-ssh	Catatan: Untuk aturan ini, pengidentifikasi aturan (INCOMING _SSH_DISABLED) dan nama aturan (restricted-ssh) berbeda. Pastikan bahwa lalu lintas SSH yang masuk untuk grup keamanan dapat diakses. Aturannya adalah COMPLIANT jika alamat IP dari lalu lintas SSH yang masuk dalam grup keamanan dibatasi (CIDR selain 0.0.0.0/0 atau: :/0). Jika tidak, NON_COMPLIANT.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	appsync-associated-with-waf	Pastikan AWS AppSync APIs yang terkait dengan daftar kontrol akses AWS WAFv2 web (ACLs). Aturannya adalah NON_COMPLIANT untuk AWS AppSync API jika tidak terkait dengan ACL web.
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber Bitbucket TIDAK berisi kredenal masuk atau tidak. Aturannya adalah NON_COMPLIANT jika URL berisi informasi login dan COMPLIANT jika tidak.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunak an sertifikat SSL yang disediaka n oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Applicati on Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	emr-block-public-access	Pastikan akun dengan Amazon EMR telah mengaktif kan pengaturan akses publik yang diblokir. Aturannya adalah NON_COMPLIANT jika BlockPublicSecurityGroupRules salah, atau jika benar, port selain Port 22 terdaftar di. PermittedPublicSecurityGroupRuleRanges
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	nacl-no-unrestricted-ssh-rdp	Pastikan port default untuk lalu lintas masuk SSH/RDP untuk daftar kontrol akses jaringan () dibatasi. NACLs Aturannya adalah NON_COMPLIANT jika entri masuk NACL memungkinkan blok sumber TCP atau UDP CIDR untuk port 22 atau 3389.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	ec2- -semua client-vpn-not-authorize	Pastikan bahwa aturan otorisasi AWS Client VPN tidak mengotorisasi akses koneksi untuk semua klien. Aturannya adalah NON_COMPLIANT jika 'AccessAll' hadir dan disetel ke true.
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	internet-gateway-authorized-vpc-hanya	Pastikan gateway internet dilampirkan ke cloud pribadi virtual resmi (Amazon VPC). Aturannya adalah NON_COMPLIANT jika gateway internet dilampirkan ke VPC yang tidak sah.
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	s3- -blok access-point-public-access	Pastikan jalur akses Amazon S3 telah mengaktifkan pengaturan akses publik blok. Aturannya adalah NON_COMPLIANT jika pengaturan akses publik blok tidak diaktifkan untuk titik akses S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	s3- -blok account-l evel-public-access	Pastikan bahwa pengaturan blok akses publik yang diperlukan dikonfigu rasi dari tingkat akun. Aturannya hanya NON_COMPLIANT jika bidang yang ditetapkan di bawah ini tidak cocok dengan bidang yang sesuai di item konfigurasi.
1.4.3	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	netfw-policy-default-action-fragmen-paket	Pastikan kebijakan AWS Network Firewall dikonfigurasi dengan tindakan default stateless yang ditentukan pengguna untuk paket terfragme ntasi. Aturannya adalah NON_COMPL IANT jika tindakan default stateless untuk paket terfragmentasi tidak cocok dengan tindakan default yang ditentukan pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.3	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	netfw-policy-default-action-fragmen-paket	Pastikan kebijakan AWS Network Firewall dikonfigurasi dengan tindakan default stateless yang ditentukan pengguna untuk paket terfragme ntasi. Aturannya adalah NON_COMPL IANT jika tindakan default stateless untuk paket terfragmentasi tidak cocok dengan tindakan default yang ditentukan pengguna.
1.4.3	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	netfw-policy-default-action-paket penuh	Pastikan kebijakan AWS Network Firewall dikonfigurasi dengan tindakan stateless default yang ditentuka n pengguna untuk paket lengkap. Aturan ini adalah NON_COMPLIANT jika tindakan stateless default untuk paket lengkap tidak cocok dengan tindakan stateless default yang ditentukan pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.4	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	api-gw-endpoint-type-periksa	Pastikan Amazon API Gateway APIs adalah tipe yang ditentuka n dalam parameter aturan 'endpoint ConfigurationType'. Aturan mengembal ikan NON_COMPL IANT jika REST API tidak cocok dengan tipe titik akhir yang dikonfigurasi dalam parameter aturan.
1.4.4	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	redshift-enhanced-vpc-routing-diaktifkan	Pastikan bahwa klaster Amazon Redshift telah 'diaktifk an. enhancedV pcRouting Aturannya adalah NON_COMPL IANT jika 'enhanced VpcRouting' tidak diaktifkan atau jika konfigurasi. enhancedVpcRouting lapangan adalah 'palsu'.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.4	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	internet-gateway-a uthorized-vpc-hanya	Pastikan gateway internet dilampirkan ke cloud pribadi virtual resmi (Amazon VPC). Aturannya adalah NON_COMPLIANT jika gateway internet dilampirkan ke VPC yang tidak sah.
1.4.5	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	ecs-task-definition-pid-mode-periksa	Pastikan bahwa ECSTask Definisi dikonfigurasi untuk berbagi namespace proses host dengan wadah Amazon Elastic Container Service (Amazon ECS). Aturannya adalah NON_COMPL IANT jika parameter PidMode disetel ke 'host'.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.5	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	ec2- launch-template-public-ip -dinonaktifkan	Pastikan Template EC2 Peluncuran Amazon tidak disetel untuk menetapkan alamat IP publik ke Antarmuka Jaringan. Aturannya adalah NON_COMPL IANT jika versi default Template EC2 Peluncuran memiliki setidaknya 1 Antarmuka Jaringan dengan '' disetel ke AssociatePublicIpA ddress 'benar'.
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	api-gw-endpoint-type-periksa	Pastikan Amazon API Gateway APIs adalah tipe yang ditentuka n dalam parameter aturan 'endpoint ConfigurationType'. Aturan mengembal ikan NON_COMPL IANT jika REST API tidak cocok dengan tipe titik akhir yang dikonfigurasi dalam parameter aturan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	netfw-policy-default-action-fragmen-paket	Pastikan kebijakan AWS Network Firewall dikonfigurasi dengan tindakan default stateless yang ditentukan pengguna untuk paket terfragmentasi. Aturannya adalah NON_COMPLIANT jika tindakan default stateless untuk paket terfragmentasi tidak cocok dengan tindakan default yang ditentukan pengguna.
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	eks-endpoint-no-public-akses	Pastikan titik akhir Amazon Elastic Kubernetes Service (Amazon EKS) tidak dapat diakses publik. Aturannya adalah NON_COMPLIANT jika titik akhir dapat diakses publik.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	terbatas-ssh	Catatan: Untuk aturan ini, pengidentifikasi aturan (INCOMING _SSH_DISABLED) dan nama aturan (restricted-ssh) berbeda. Pastikan bahwa lalu lintas SSH yang masuk untuk grup keamanan dapat diakses. Aturannya adalah COMPLIANT jika alamat IP dari lalu lintas SSH yang masuk dalam grup keamanan dibatasi (CIDR selain 0.0.0.0/0 atau: :/0). Jika tidak, NON_COMPLIANT.
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	appsync-associated-with-waf	Pastikan AWS AppSync APIs yang terkait dengan daftar kontrol akses AWS WAFv2 web (ACLs). Aturannya adalah NON_COMPLIANT untuk AWS AppSync API jika tidak terkait dengan ACL web.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber Bitbucket TIDAK berisi kredenal masuk atau tidak. Aturannya adalah NON_COMPLIANT jika URL berisi informasi login dan COMPLIANT jika tidak.
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	emr-block-public-access	Pastikan akun dengan Amazon EMR telah mengaktifkan pengaturan akses publik yang diblokir. Aturannya adalah NON_COMPLIANT jika BlockPublicSecurityGroupRules salah, atau jika benar, port selain Port 22 terdaftar di. PermittedPublicSecurityGroupRuleRanges
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	nacl-no-unrestricted-ssh-rdp	Pastikan port default untuk lalu lintas masuk SSH/RDP untuk daftar kontrol akses jaringan () dibatasi. NACLs Aturannya adalah NON_COMPLIANT jika entri masuk NACL memungkinkan blok sumber TCP atau UDP CIDR untuk port 22 atau 3389.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	ec2- -semua client-vpn-not-authorize	Pastikan bahwa aturan otorisasi AWS Client VPN tidak mengotorisasi akses koneksi untuk semua klien. Aturannya adalah NON_COMPLIANT jika 'AccessAll' hadir dan disetel ke true.
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	internet-gateway-authorized-vpc-hanya	Pastikan gateway internet dilampirkan ke cloud pribadi virtual resmi (Amazon VPC). Aturannya adalah NON_COMPLIANT jika gateway internet dilampirkan ke VPC yang tidak sah.
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	s3- -blok access-point-public-access	Pastikan jalur akses Amazon S3 telah mengaktifkan pengaturan akses publik blok. Aturannya adalah NON_COMPLIANT jika pengaturan akses publik blok tidak diaktifkan untuk titik akses S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	s3- -blok account-level-public-access	Pastikan bahwa pengaturan blok akses publik yang diperlukan dikonfigurasi dari tingkat akun. Aturannya hanya NON_COMPLIANT jika bidang yang ditetapkan di bawah ini tidak cocok dengan bidang yang sesuai di item konfigurasi.
10.2.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gwv2- access-logs-enabled	Pastikan bahwa tahap Amazon API Gateway V2 mengaktifkan pencatatan akses. Aturannya adalah NON_COMPLIANT jika 'accessLogSettings' tidak ada dalam konfigurasi Stage.
10.2.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	neptune-cluster-cloudwatch-log-ekspor diaktifkan	Pastikan klaster CloudWatch Amazon Neptunus mengaktifkan ekspor log untuk log audit. Aturannya adalah NON_COMPLIANT jika cluster Neptunus tidak mengaktifkan ekspor log untuk log audit. CloudWatch
10.2.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	ecs-task-definition-log-konfigurasi	Pastikan bahwa LogConfiguration diatur pada Definisi Tugas ECS aktif. Aturan ini NON_COMPLIANT jika ECSTask Definisi aktif tidak memiliki sumber daya LogConfiguration yang ditentukan atau nilai untuk LogConfiguration adalah null dalam setidaknya satu definisi kontainer.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudtrail-diaktifkan	Catatan: Untuk aturan ini, pengidentifikasi aturan (CLOUD_TRAIL_ENABLED) dan nama aturan (cloudtrail-enabled) berbeda. Pastikan AWS CloudTrail jejak diaktifkan di AWS akun Anda. Aturannya adalah NON_COMPLIANT jika jejak tidak diaktifkan. Secara opsional, aturan memeriksa bucket S3 tertentu, topik Amazon Simple Notification Service (Amazon SNS), dan grup log. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	multi-region-cloudtrail-enabled	Catatan: untuk aturan ini, pengidentifikasi aturan (MULTI_REGION_CLOUD_TRAIL_ENABLED) dan nama aturan () berbeda. multi-region-cloudtrail-enabled Pastikan setidaknya ada satu multi-wilayah AWS CloudTrail. Aturannya adalah NON_COMPLIANT jika jejak tidak cocok dengan parameter input. Aturannya adalah NON_COMPLIANT jika ExcludeManagementEventSources bidang tidak kosong atau jika AWS CloudTrail dikonfigurasi untuk mengecualikan peristiwa manajemen seperti peristiwa AWS KMS atau peristiwa API Data Amazon RDS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	appsync-logging-enabled	Pastikan bahwa AWS AppSync API telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan, atau 'fieldLogLevel' bukan ERROR atau SEMUA.
10.2.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-logging-diaktifkan	Pastikan pialang Amazon MQ mengaktifkan pencatatan CloudWatch audit Amazon. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.
10.2.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-log-diaktifkan	Pastikan bahwa broker Amazon MQ mengaktifkan pencatatan CloudWatch audit. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	eks-cluster-logging-enabled	Pastikan klaster Amazon Elastic Kubernetes Service (Amazon EKS) dikonfigurasi dengan logging diaktifkan. Aturannya adalah NON_COMPLIANT jika logging untuk klaster Amazon EKS tidak diaktifkan untuk semua jenis log.
10.2.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	elastic-beanstalk-logs-to-jam tangan awan	Pastikan lingkungan AWS Elastic Beanstalk dikonfigurasi untuk mengirim log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika nilai `StreamLogs` salah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	step-functions-state-machine-logging-diaktifkan	Pastikan bahwa mesin AWS Step Functions telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika mesin status tidak mengaktifkan logging atau konfigurasi logging tidak pada tingkat minimum yang disediakan.
10.2.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	netfw-logging-enabled	Pastikan firewall AWS Network Firewall telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika jenis logging tidak dikonfigurasi. Anda dapat menentukan jenis logging yang Anda ingin aturan untuk memeriksa.
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gwv2- access-logs-enabled	Pastikan bahwa tahap Amazon API Gateway V2 mengaktifkan pencatatan akses. Aturannya adalah NON_COMPLIANT jika 'accessLogSettings' tidak ada dalam konfigurasi Stage.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	neptune-cluster-cloudwatch-log-ekspor diaktifkan	Pastikan klaster CloudWatch Amazon Neptunus mengaktifkan ekspor log untuk log audit. Aturannya adalah NON_COMPLIANT jika cluster Neptunus tidak mengaktifkan ekspor log untuk log audit. CloudWatch
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	ec2- instance-detailed-monitoring-enabled	Pastikan pemantauan terperinci diaktifkan untuk EC2 instans. Aturannya adalah NON_COMPLIANT jika pemantauan terperinci tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	ecs-task-definition-log-konfigurasi	Pastikan bahwa LogConfiguration diatur pada Definisi Tugas ECS aktif. Aturan ini NON_COMPLIANT jika ECSTask Definisi aktif tidak memiliki sumber daya LogConfiguration yang ditentukan atau nilai untuk LogConfiguration adalah null dalam setidaknya satu definisi kontainer.
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudwatch-alarm-resource-check	Pastikan bahwa jenis sumber daya memiliki CloudWatch alarm untuk metrik bernama. Untuk jenis sumber daya, Anda dapat menentukan volume EBS, EC2 instans, kluster Amazon RDS, atau bucket S3. Aturannya adalah COMPLIANT jika metrik bernama memiliki ID sumber daya dan CloudWatch alarm.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudtrail-diaktifkan	Catatan: Untuk aturan ini, pengidentifikasi aturan (CLOUD_TRAIL_ENABLED) dan nama aturan (cloudtrail-enabled) berbeda. Pastikan AWS CloudTrail jejak diaktifkan di AWS akun Anda. Aturannya adalah NON_COMPLIANT jika jejak tidak diaktifkan. Secara opsional, aturan memeriksa bucket S3 tertentu, topik Amazon Simple Notification Service (Amazon SNS), dan grup log. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	multi-region-cloudtrail-enabled	Catatan: untuk aturan ini, pengidentifikasi aturan (MULTI_REGION_CLOUD_TRAIL_ENABLED) dan nama aturan () berbeda. multi-region-cloudtrail-enabled Pastikan setidaknya ada satu multi-wilayah AWS CloudTrail. Aturannya adalah NON_COMPLIANT jika jejak tidak cocok dengan parameter input. Aturannya adalah NON_COMPLIANT jika ExcludeManagementEventSources bidang tidak kosong atau jika AWS CloudTrail dikonfigurasi untuk mengecualikan peristiwa manajemen seperti peristiwa AWS KMS atau peristiwa API Data Amazon RDS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	appsync-logging-enabled	Pastikan bahwa AWS AppSync API telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan, atau 'fieldLogLevel' bukan ERROR atau SEMUA.
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-logging-diaktifkan	Pastikan pialang Amazon MQ mengaktifkan pencatatan CloudWatch audit Amazon. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-log-diaktifkan	Pastikan bahwa broker Amazon MQ mengaktifkan pencatatan CloudWatch audit. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	eks-cluster-logging-enabled	Pastikan klaster Amazon Elastic Kubernetes Service (Amazon EKS) dikonfigurasi dengan logging diaktifkan. Aturannya adalah NON_COMPLIANT jika logging untuk klaster Amazon EKS tidak diaktifkan untuk semua jenis log.
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	elastic-beanstalk-logs-to-jam tangan awan	Pastikan lingkungan AWS Elastic Beanstalk dikonfigurasi untuk mengirim log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika nilai `StreamLogs` salah.
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	wafv2- rulegroup-logging-enabled	Pastikan pengumpulan metrik CloudWatch keamanan Amazon pada grup AWS WAFv2 aturan diaktifkan. Aturannya adalah NON_COMPLIANT jika '. VisibilityConfig CloudWatchMetricsEnabled'bidang disetel ke false.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	sns-topic-message-delivery-notifikasi-diaktifkan	Pastikan pencatatan Amazon Simple Notification Service (SNS) diaktifkan untuk status pengiriman pesan notifikasi yang dikirim ke topik untuk titik akhir. Aturannya adalah NON_COMPLIANT jika pemberitahuan status pengiriman untuk pesan tidak diaktifkan.
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	step-functions-state-machine-logging-diaktifkan	Pastikan bahwa mesin AWS Step Functions telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika mesin status tidak mengaktifkan logging atau konfigurasi logging tidak pada tingkat minimum yang disediakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	netfw-logging-enabled	Pastikan firewall AWS Network Firewall telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika jenis logging tidak dikonfigurasi. Anda dapat menentukan jenis logging yang Anda ingin aturan untuk memeriksa.
10.2.1.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gwv2- access-logs-enabled	Pastikan bahwa tahap Amazon API Gateway V2 mengaktifkan pencatatan akses. Aturannya adalah NON_COMPLIANT jika 'accessLogSettings' tidak ada dalam konfigurasi Stage.
10.2.1.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	neptune-cluster-cloudwatch-log-ekspor diaktifkan	Pastikan klaster CloudWatch Amazon Neptunus mengaktifkan ekspor log untuk log audit. Aturannya adalah NON_COMPLIANT jika cluster Neptunus tidak mengaktifkan ekspor log untuk log audit. CloudWatch
10.2.1.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	ecs-task-definition-log-konfigurasi	Pastikan bahwa LogConfiguration diatur pada Definisi Tugas ECS aktif. Aturan ini NON_COMPLIANT jika ECSTask Definisi aktif tidak memiliki sumber daya LogConfiguration yang ditentukan atau nilai untuk LogConfiguration adalah null dalam setidaknya satu definisi kontainer.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudtrail-diaktifkan	Catatan: Untuk aturan ini, pengidentifikasi aturan (CLOUD_TRAIL_ENABLED) dan nama aturan (cloudtrail-enabled) berbeda. Pastikan AWS CloudTrail jejak diaktifkan di AWS akun Anda. Aturannya adalah NON_COMPLIANT jika jejak tidak diaktifkan. Secara opsional, aturan memeriksa bucket S3 tertentu, topik Amazon Simple Notification Service (Amazon SNS), dan grup log. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	multi-region-cloudtrail-enabled	Catatan: untuk aturan ini, pengidentifikasi aturan (MULTI_REGION_CLOUD_TRAIL_ENABLED) dan nama aturan () berbeda. multi-region-cloudtrail-enabled Pastikan setidaknya ada satu multi-wilayah AWS CloudTrail. Aturannya adalah NON_COMPLIANT jika jejak tidak cocok dengan parameter input. Aturannya adalah NON_COMPLIANT jika ExcludeManagementEventSources bidang tidak kosong atau jika AWS CloudTrail dikonfigurasi untuk mengecualikan peristiwa manajemen seperti peristiwa AWS KMS atau peristiwa API Data Amazon RDS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	appsync-logging-enabled	Pastikan bahwa AWS AppSync API telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan, atau 'fieldLogLevel' bukan ERROR atau SEMUA.
10.2.1.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-logging-diaktifkan	Pastikan pialang Amazon MQ mengaktifkan pencatatan CloudWatch audit Amazon. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.
10.2.1.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-log-diaktifkan	Pastikan bahwa broker Amazon MQ mengaktifkan pencatatan CloudWatch audit. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	eks-cluster-logging-enabled	Pastikan klaster Amazon Elastic Kubernetes Service (Amazon EKS) dikonfigurasi dengan logging diaktifkan. Aturannya adalah NON_COMPLIANT jika logging untuk klaster Amazon EKS tidak diaktifkan untuk semua jenis log.
10.2.1.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	elastic-beanstalk-logs-to-jam tangan awan	Pastikan lingkungan AWS Elastic Beanstalk dikonfigurasi untuk mengirim log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika nilai `StreamLogs` salah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	step-functions-state-machine-logging-diaktifkan	Pastikan bahwa mesin AWS Step Functions telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika mesin status tidak mengaktifkan logging atau konfigurasi logging tidak pada tingkat minimum yang disediakan.
10.2.1.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	netfw-logging-enabled	Pastikan firewall AWS Network Firewall telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika jenis logging tidak dikonfigurasi. Anda dapat menentukan jenis logging yang Anda ingin aturan untuk memeriksa.
10.2.1.3	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gwv2- access-logs-enabled	Pastikan bahwa tahap Amazon API Gateway V2 mengaktifkan pencatatan akses. Aturannya adalah NON_COMPLIANT jika 'accessLogSettings' tidak ada dalam konfigurasi Stage.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.3	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
10.2.1.3	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	neptune-cluster-cloudwatch-log-ekspor diaktifkan	Pastikan klaster CloudWatch Amazon Neptunus mengaktifkan ekspor log untuk log audit. Aturannya adalah NON_COMPLIANT jika cluster Neptunus tidak mengaktifkan ekspor log untuk log audit. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.3	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	ecs-task-definition-log-konfigurasi	Pastikan bahwa LogConfiguration diatur pada Definisi Tugas ECS aktif. Aturan ini NON_COMPLIANT jika ECSTask Definisi aktif tidak memiliki sumber daya LogConfiguration yang ditentukan atau nilai untuk LogConfiguration adalah null dalam setidaknya satu definisi kontainer.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.3	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudtrail-diaktifkan	Catatan: Untuk aturan ini, pengidentifikasi aturan (CLOUD_TRAIL_ENABLED) dan nama aturan (cloudtrail-enabled) berbeda. Pastikan AWS CloudTrail jejak diaktifkan di AWS akun Anda. Aturannya adalah NON_COMPLIANT jika jejak tidak diaktifkan. Secara opsional, aturan memeriksa bucket S3 tertentu, topik Amazon Simple Notification Service (Amazon SNS), dan grup log. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.3	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	multi-region-cloudtrail-enabled	Catatan: untuk aturan ini, pengidentifikasi aturan (MULTI_REGION_CLOUD_TRAIL_ENABLED) dan nama aturan () berbeda. multi-region-cloudtrail-enabled Pastikan setidaknya ada satu multi-wilayah AWS CloudTrail. Aturannya adalah NON_COMPLIANT jika jejak tidak cocok dengan parameter input. Aturannya adalah NON_COMPLIANT jika ExcludeManagementEventSources bidang tidak kosong atau jika AWS CloudTrail dikonfigurasi untuk mengecualikan peristiwa manajemen seperti peristiwa AWS KMS atau peristiwa API Data Amazon RDS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.3	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	appsync-logging-enabled	Pastikan bahwa AWS AppSync API telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan, atau 'fieldLogLevel' bukan ERROR atau SEMUA.
10.2.1.3	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-logging-diaktifkan	Pastikan pialang Amazon MQ mengaktifkan pencatatan CloudWatch audit Amazon. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.
10.2.1.3	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-log-diaktifkan	Pastikan bahwa broker Amazon MQ mengaktifkan pencatatan CloudWatch audit. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.3	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	eks-cluster-logging-enabled	Pastikan klaster Amazon Elastic Kubernetes Service (Amazon EKS) dikonfigurasi dengan logging diaktifkan. Aturannya adalah NON_COMPLIANT jika logging untuk klaster Amazon EKS tidak diaktifkan untuk semua jenis log.
10.2.1.3	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	elastic-beanstalk-logs-to-jam tangan awan	Pastikan lingkungan AWS Elastic Beanstalk dikonfigurasi untuk mengirim log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika nilai `StreamLogs` salah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.3	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	step-functions-state-machine-logging-diaktifkan	Pastikan bahwa mesin AWS Step Functions telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika mesin status tidak mengaktifkan logging atau konfigurasi logging tidak pada tingkat minimum yang disediakan.
10.2.1.3	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	netfw-logging-enabled	Pastikan firewall AWS Network Firewall telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika jenis logging tidak dikonfigurasi. Anda dapat menentukan jenis logging yang Anda ingin aturan untuk memeriksa.
10.2.1.4	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gwv2- access-logs-enabled	Pastikan tahap Amazon API Gateway V2 mengaktifkan pencatatan akses. Aturannya adalah NON_COMPLIANT jika 'accessLogSettings' tidak ada dalam konfigurasi Stage.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.4	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
10.2.1.4	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	neptune-cluster-cloudwatch-log-ekspor diaktifkan	Pastikan klaster CloudWatch Amazon Neptunus mengaktifkan ekspor log untuk log audit. Aturannya adalah NON_COMPLIANT jika klaster Neptunus tidak mengaktifkan ekspor log untuk log audit. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.4	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	ecs-task-definition-log-konfigurasi	Pastikan bahwa LogConfiguration diatur pada Definisi Tugas ECS aktif. Aturan ini NON_COMPLIANT jika ECSTask Definisi aktif tidak memiliki sumber daya LogConfiguration yang ditentukan atau nilai untuk LogConfiguration adalah null dalam setidaknya satu definisi kontainer.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.4	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudtrail-diaktifkan	Catatan: Untuk aturan ini, pengidentifikasi aturan (CLOUD_TRAIL_ENABLED) dan nama aturan (cloudtrail-enabled) berbeda. Pastikan AWS CloudTrail jejak diaktifkan di AWS akun Anda. Aturannya adalah NON_COMPLIANT jika jejak tidak diaktifkan. Secara opsional, aturan memeriksa bucket S3 tertentu, topik Amazon Simple Notification Service (Amazon SNS), dan grup log. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.4	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	multi-region-cloudtrail-enabled	Catatan: untuk aturan ini, pengidentifikasi aturan (MULTI_REGION_CLOUD_TRAIL_ENABLED) dan nama aturan () berbeda. multi-region-cloudtrail-enabled Pastikan setidaknya ada satu multi-wilayah AWS CloudTrail. Aturannya adalah NON_COMPLIANT jika jejak tidak cocok dengan parameter input. Aturannya adalah NON_COMPLIANT jika ExcludeManagementEventSources bidang tidak kosong atau jika AWS CloudTrail dikonfigurasi untuk mengecualikan peristiwa manajemen seperti peristiwa AWS KMS atau peristiwa API Data Amazon RDS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.4	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	appsync-logging-enabled	Pastikan bahwa AWS AppSync API telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan, atau 'fieldLogLevel' bukan ERROR atau SEMUA.
10.2.1.4	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-logging-diaktifkan	Pastikan pialang Amazon MQ mengaktifkan pencatatan CloudWatch audit Amazon. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.
10.2.1.4	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-log-diaktifkan	Pastikan bahwa broker Amazon MQ mengaktifkan pencatatan CloudWatch audit. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.4	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	eks-cluster-logging-enabled	Pastikan klaster Amazon Elastic Kubernetes Service (Amazon EKS) dikonfigurasi dengan logging diaktifkan. Aturannya adalah NON_COMPLIANT jika logging untuk klaster Amazon EKS tidak diaktifkan untuk semua jenis log.
10.2.1.4	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	elastic-beanstalk-logs-to-jam tangan awan	Pastikan lingkungan AWS Elastic Beanstalk dikonfigurasi untuk mengirim log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika nilai `StreamLogs` salah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.4	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	step-functions-state-machine-logging-diaktifkan	Pastikan bahwa mesin AWS Step Functions telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika mesin status tidak mengaktifkan logging atau konfigurasi logging tidak pada tingkat minimum yang disediakan.
10.2.1.4	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	netfw-logging-enabled	Pastikan firewall AWS Network Firewall telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika jenis logging tidak dikonfigurasi. Anda dapat menentukan jenis logging yang Anda ingin aturan untuk memeriksa.
10.2.1.5	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gwv2- access-logs-enabled	Pastikan tahap Amazon API Gateway V2 mengaktifkan pencatatan akses. Aturannya adalah NON_COMPLIANT jika 'accessLogSettings' tidak ada dalam konfigurasi Stage.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.5	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
10.2.1.5	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	neptune-cluster-cloudwatch-log-ekspor diaktifkan	Pastikan klaster CloudWatch Amazon Neptunus mengaktifkan ekspor log untuk log audit. Aturannya adalah NON_COMPLIANT jika klaster Neptunus tidak mengaktifkan ekspor log untuk log audit. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.5	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	ecs-task-definition-log-konfigurasi	Pastikan bahwa LogConfiguration diatur pada Definisi Tugas ECS aktif. Aturan ini NON_COMPLIANT jika ECSTask Definisi aktif tidak memiliki sumber daya LogConfiguration yang ditentukan atau nilai untuk LogConfiguration adalah null dalam setidaknya satu definisi kontainer.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.5	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudtrail-diaktifkan	Catatan: Untuk aturan ini, pengidentifikasi aturan (CLOUD_TRAIL_ENABLED) dan nama aturan (cloudtrail-enabled) berbeda. Pastikan AWS CloudTrail jejak diaktifkan di AWS akun Anda. Aturannya adalah NON_COMPLIANT jika jejak tidak diaktifkan. Secara opsional, aturan memeriksa bucket S3 tertentu, topik Amazon Simple Notification Service (Amazon SNS), dan grup log. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.5	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	multi-region-cloudtrail-enabled	Catatan: untuk aturan ini, pengidentifikasi aturan (MULTI_REGION_CLOUD_TRAIL_ENABLED) dan nama aturan () berbeda. multi-region-cloudtrail-enabled Pastikan setidaknya ada satu multi-wilayah AWS CloudTrail. Aturannya adalah NON_COMPLIANT jika jejak tidak cocok dengan parameter input. Aturannya adalah NON_COMPLIANT jika ExcludeManagementEventSources bidang tidak kosong atau jika AWS CloudTrail dikonfigurasi untuk mengecualikan peristiwa manajemen seperti peristiwa AWS KMS atau peristiwa API Data Amazon RDS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.5	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	appsync-logging-enabled	Pastikan bahwa AWS AppSync API telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan, atau 'fieldLogLevel' bukan ERROR atau SEMUA.
10.2.1.5	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-logging-diaktifkan	Pastikan pialang Amazon MQ mengaktifkan pencatatan CloudWatch audit Amazon. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.
10.2.1.5	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-log-diaktifkan	Pastikan bahwa broker Amazon MQ mengaktifkan pencatatan CloudWatch audit. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.5	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	eks-cluster-logging-enabled	Pastikan klaster Amazon Elastic Kubernetes Service (Amazon EKS) dikonfigurasi dengan logging diaktifkan. Aturannya adalah NON_COMPLIANT jika logging untuk klaster Amazon EKS tidak diaktifkan untuk semua jenis log.
10.2.1.5	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	elastic-beanstalk-logs-to-jam tangan awan	Pastikan lingkungan AWS Elastic Beanstalk dikonfigurasi untuk mengirim log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika nilai `StreamLogs` salah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.5	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	step-functions-state-machine-logging-diaktifkan	Pastikan bahwa mesin AWS Step Functions telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika mesin status tidak mengaktifkan logging atau konfigurasi logging tidak pada tingkat minimum yang disediakan.
10.2.1.5	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	netfw-logging-enabled	Pastikan firewall AWS Network Firewall telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika jenis logging tidak dikonfigurasi. Anda dapat menentukan jenis logging yang Anda ingin aturan untuk memeriksa.
10.2.1.6	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gwv2- access-logs-enabled	Pastikan tahap Amazon API Gateway V2 mengaktifkan pencatatan akses. Aturannya adalah NON_COMPLIANT jika 'accessLogSettings' tidak ada dalam konfigurasi Stage.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.6	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
10.2.1.6	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	neptune-cluster-cloudwatch-log-ekspor diaktifkan	Pastikan klaster CloudWatch Amazon Neptunus mengaktifkan ekspor log untuk log audit. Aturannya adalah NON_COMPLIANT jika klaster Neptunus tidak mengaktifkan ekspor log untuk log audit. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.6	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	ecs-task-definition-log-konfigurasi	Pastikan bahwa LogConfiguration diatur pada Definisi Tugas ECS aktif. Aturan ini NON_COMPLIANT jika ECSTask Definisi aktif tidak memiliki sumber daya LogConfiguration yang ditentukan atau nilai untuk LogConfiguration adalah null dalam setidaknya satu definisi kontainer.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.6	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudtrail-diaktifkan	Catatan: Untuk aturan ini, pengidentifikasi aturan (CLOUD_TRAIL_ENABLED) dan nama aturan (cloudtrail-enabled) berbeda. Pastikan AWS CloudTrail jejak diaktifkan di AWS akun Anda. Aturannya adalah NON_COMPLIANT jika jejak tidak diaktifkan. Secara opsional, aturan memeriksa bucket S3 tertentu, topik Amazon Simple Notification Service (Amazon SNS), dan grup log. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.6	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	multi-region-cloudtrail-enabled	Catatan: untuk aturan ini, pengidentifikasi aturan (MULTI_REGION_CLOUD_TRAIL_ENABLED) dan nama aturan () berbeda. multi-region-cloudtrail-enabled Pastikan setidaknya ada satu multi-wilayah AWS CloudTrail. Aturannya adalah NON_COMPLIANT jika jejak tidak cocok dengan parameter input. Aturannya adalah NON_COMPLIANT jika ExcludeManagementEventSources bidang tidak kosong atau jika AWS CloudTrail dikonfigurasi untuk mengecualikan peristiwa manajemen seperti peristiwa AWS KMS atau peristiwa API Data Amazon RDS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.6	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	appsync-logging-enabled	Pastikan bahwa AWS AppSync API telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan, atau 'fieldLogLevel' bukan ERROR atau SEMUA.
10.2.1.6	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-logging-diaktifkan	Pastikan pialang Amazon MQ mengaktifkan pencatatan CloudWatch audit Amazon. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.
10.2.1.6	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-log-diaktifkan	Pastikan bahwa broker Amazon MQ mengaktifkan pencatatan CloudWatch audit. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.6	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	eks-cluster-logging-enabled	Pastikan klaster Amazon Elastic Kubernetes Service (Amazon EKS) dikonfigurasi dengan logging diaktifkan. Aturannya adalah NON_COMPLIANT jika logging untuk klaster Amazon EKS tidak diaktifkan untuk semua jenis log.
10.2.1.6	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	elastic-beanstalk-logs-to-jam tangan awan	Pastikan lingkungan AWS Elastic Beanstalk dikonfigurasi untuk mengirim log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika nilai `StreamLogs` salah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.6	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	step-functions-state-machine-logging-diaktifkan	Pastikan bahwa mesin AWS Step Functions telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika mesin status tidak mengaktifkan logging atau konfigurasi logging tidak pada tingkat minimum yang disediakan.
10.2.1.6	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	netfw-logging-enabled	Pastikan firewall AWS Network Firewall telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika jenis logging tidak dikonfigurasi. Anda dapat menentukan jenis logging yang Anda ingin aturan untuk memeriksa.
10.2.1.7	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gwv2- access-logs-enabled	Pastikan tahap Amazon API Gateway V2 mengaktifkan pencatatan akses. Aturannya adalah NON_COMPLIANT jika 'accessLogSettings' tidak ada dalam konfigurasi Stage.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.7	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
10.2.1.7	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	neptune-cluster-cloudwatch-log-ekspor diaktifkan	Pastikan klaster CloudWatch Amazon Neptunus mengaktifkan ekspor log untuk log audit. Aturannya adalah NON_COMPLIANT jika klaster Neptunus tidak mengaktifkan ekspor log untuk log audit. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.7	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	ecs-task-definition-log-konfigurasi	Pastikan bahwa LogConfiguration diatur pada Definisi Tugas ECS aktif. Aturan ini NON_COMPLIANT jika ECSTask Definisi aktif tidak memiliki sumber daya LogConfiguration yang ditentukan atau nilai untuk LogConfiguration adalah null dalam setidaknya satu definisi kontainer.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.7	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudtrail-diaktifkan	Catatan: Untuk aturan ini, pengidentifikasi aturan (CLOUD_TRAIL_ENABLED) dan nama aturan (cloudtrail-enabled) berbeda. Pastikan AWS CloudTrail jejak diaktifkan di AWS akun Anda. Aturannya adalah NON_COMPLIANT jika jejak tidak diaktifkan. Secara opsional, aturan memeriksa bucket S3 tertentu, topik Amazon Simple Notification Service (Amazon SNS), dan grup log. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.7	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	multi-region-cloudtrail-enabled	Catatan: untuk aturan ini, pengidentifikasi aturan (MULTI_REGION_CLOUD_TRAIL_ENABLED) dan nama aturan () berbeda. multi-region-cloudtrail-enabled Pastikan setidaknya ada satu multi-wilayah AWS CloudTrail. Aturannya adalah NON_COMPLIANT jika jejak tidak cocok dengan parameter input. Aturannya adalah NON_COMPLIANT jika ExcludeManagementEventSources bidang tidak kosong atau jika AWS CloudTrail dikonfigurasi untuk mengecualikan peristiwa manajemen seperti peristiwa AWS KMS atau peristiwa API Data Amazon RDS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.7	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	appsync-logging-enabled	Pastikan bahwa AWS AppSync API telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan, atau 'fieldLogLevel' bukan ERROR atau SEMUA.
10.2.1.7	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-logging-diaktifkan	Pastikan pialang Amazon MQ mengaktifkan pencatatan CloudWatch audit Amazon. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.
10.2.1.7	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-log-diaktifkan	Pastikan bahwa broker Amazon MQ mengaktifkan pencatatan CloudWatch audit. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.7	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	eks-cluster-logging-enabled	Pastikan klaster Amazon Elastic Kubernetes Service (Amazon EKS) dikonfigurasi dengan logging diaktifkan. Aturannya adalah NON_COMPLIANT jika logging untuk klaster Amazon EKS tidak diaktifkan untuk semua jenis log.
10.2.1.7	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	elastic-beanstalk-logs-to-jam tangan awan	Pastikan lingkungan AWS Elastic Beanstalk dikonfigurasi untuk mengirim log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika nilai `StreamLogs` salah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.7	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	step-functions-state-machine-logging-diaktifkan	Pastikan bahwa mesin AWS Step Functions telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika mesin status tidak mengaktifkan logging atau konfigurasi logging tidak pada tingkat minimum yang disediakan.
10.2.1.7	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	netfw-logging-enabled	Pastikan firewall AWS Network Firewall telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika jenis logging tidak dikonfigurasi. Anda dapat menentukan jenis logging yang Anda ingin aturan untuk memeriksa.
10.2.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gwv2- access-logs-enabled	Pastikan tahap Amazon API Gateway V2 mengaktifkan pencatatan akses. Aturannya adalah NON_COMPLIANT jika 'accessLogSettings' tidak ada dalam konfigurasi Stage.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
10.2.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	neptune-cluster-cloudwatch-log-ekspor diaktifkan	Pastikan klaster CloudWatch Amazon Neptunus mengaktifkan ekspor log untuk log audit. Aturannya adalah NON_COMPLIANT jika klaster Neptunus tidak mengaktifkan ekspor log untuk log audit. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	ecs-task-definition-log-konfigurasi	Pastikan bahwa LogConfiguration diatur pada Definisi Tugas ECS aktif. Aturan ini NON_COMPLIANT jika ECSTask Definisi aktif tidak memiliki sumber daya LogConfiguration yang ditentukan atau nilai untuk LogConfiguration adalah null dalam setidaknya satu definisi kontainer.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudtrail-diaktifkan	Catatan: Untuk aturan ini, pengidentifikasi aturan (CLOUD_TRAIL_ENABLED) dan nama aturan (cloudtrail-enabled) berbeda. Pastikan AWS CloudTrail jejak diaktifkan di AWS akun Anda. Aturannya adalah NON_COMPLIANT jika jejak tidak diaktifkan. Secara opsional, aturan memeriksa bucket S3 tertentu, topik Amazon Simple Notification Service (Amazon SNS), dan grup log. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	multi-region-cloudtrail-enabled	Catatan: untuk aturan ini, pengidentifikasi aturan (MULTI_REGION_CLOUD_TRAIL_ENABLED) dan nama aturan () berbeda. multi-region-cloudtrail-enabled Pastikan setidaknya ada satu multi-wilayah AWS CloudTrail. Aturannya adalah NON_COMPLIANT jika jejak tidak cocok dengan parameter input. Aturannya adalah NON_COMPLIANT jika ExcludeManagementEventSources bidang tidak kosong atau jika AWS CloudTrail dikonfigurasi untuk mengecualikan peristiwa manajemen seperti peristiwa AWS KMS atau peristiwa API Data Amazon RDS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	appsync-logging-enabled	Pastikan bahwa AWS AppSync API telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan, atau 'fieldLogLevel' bukan ERROR atau SEMUA.
10.2.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-logging-diaktifkan	Pastikan pialang Amazon MQ mengaktifkan pencatatan CloudWatch audit Amazon. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.
10.2.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-log-diaktifkan	Pastikan bahwa broker Amazon MQ mengaktifkan pencatatan CloudWatch audit. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	eks-cluster-logging-enabled	Pastikan klaster Amazon Elastic Kubernetes Service (Amazon EKS) dikonfigurasi dengan logging diaktifkan. Aturannya adalah NON_COMPLIANT jika logging untuk klaster Amazon EKS tidak diaktifkan untuk semua jenis log.
10.2.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	elastic-beanstalk-logs-to-jam tangan awan	Pastikan lingkungan AWS Elastic Beanstalk dikonfigurasi untuk mengirim log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika nilai `StreamLogs` salah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	step-functions-state-machine-logging-diaktifkan	Pastikan bahwa mesin AWS Step Functions telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika mesin status tidak mengaktifkan logging atau konfigurasi logging tidak pada tingkat minimum yang disediakan.
10.2.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	netfw-logging-enabled	Pastikan firewall AWS Network Firewall telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika jenis logging tidak dikonfigurasi. Anda dapat menentukan jenis logging yang Anda ingin aturan untuk memeriksa.
10.3.1	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	api-gwv2- access-logs-enabled	Pastikan tahap Amazon API Gateway V2 mengaktifkan pencatatan akses. Aturannya adalah NON_COMPLIANT jika 'accessLogSettings' tidak ada dalam konfigurasi Stage.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.1	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
10.3.1	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	neptune-cluster-cloudwatch-log-ekspor diaktifkan	Pastikan klaster CloudWatch Amazon Neptunus mengaktifkan ekspor log untuk log audit. Aturannya adalah NON_COMPLIANT jika klaster Neptunus tidak mengaktifkan ekspor log untuk log audit. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.1	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	ecs-task-definition-log-konfigurasi	Pastikan bahwa LogConfiguration diatur pada Definisi Tugas ECS aktif. Aturan ini NON_COMPL IANT jika ECSTask Definisi aktif tidak memiliki sumber daya LogConfiguration yang ditentukan atau nilai untuk LogConfig uration adalah null dalam setidaknya satu definisi kontainer.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.1	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	cloudtrail-diaktifkan	Catatan: Untuk aturan ini, pengidentifikasi aturan (CLOUD_TRAIL_ENABLED) dan nama aturan (cloudtrail-enabled) berbeda. Pastikan AWS CloudTrail jejak diaktifkan di AWS akun Anda. Aturannya adalah NON_COMPLIANT jika jejak tidak diaktifkan. Secara opsional, aturan memeriksa bucket S3 tertentu, topik Amazon Simple Notification Service (Amazon SNS), dan grup log. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.1	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	multi-region-cloudtrail-enabled	Catatan: untuk aturan ini, pengidentifikasi aturan (MULTI_REGION_CLOUD_TRAIL_ENABLED) dan nama aturan () berbeda. multi-region-cloudtrail-enabled Pastikan setidaknya ada satu multi-wilayah AWS CloudTrail. Aturannya adalah NON_COMPLIANT jika jejak tidak cocok dengan parameter input. Aturannya adalah NON_COMPLIANT jika ExcludeManagementEventSources bidang tidak kosong atau jika AWS CloudTrail dikonfigurasi untuk mengecualikan peristiwa manajemen seperti peristiwa AWS KMS atau peristiwa API Data Amazon RDS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.1	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	appsync-logging-enabled	Pastikan bahwa AWS AppSync API telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan, atau 'fieldLogLevel' bukan ERROR atau SEMUA.
10.3.1	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	mq-cloudwatch-audit-logging-diaktifkan	Pastikan pialang Amazon MQ mengaktifkan pencatatan CloudWatch audit Amazon. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.
10.3.1	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	mq-cloudwatch-audit-log-diaktifkan	Pastikan bahwa broker Amazon MQ mengaktif kan pencatatan CloudWatch audit. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.1	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	eks-cluster-logging-enabled	Pastikan klaster Amazon Elastic Kubernetes Service (Amazon EKS) dikonfigurasi dengan logging diaktifkan. Aturannya adalah NON_COMPLIANT jika logging untuk klaster Amazon EKS tidak diaktifkan untuk semua jenis log.
10.3.1	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	elastic-beanstalk-logs-to-jam tangan awan	Pastikan lingkungan AWS Elastic Beanstalk dikonfigurasi untuk mengirim log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika nilai `StreamLogs` salah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.1	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	step-functions-state-machine-logging-diaktifkan	Pastikan bahwa mesin AWS Step Functions telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika mesin status tidak mengaktifkan logging atau konfigurasi logging tidak pada tingkat minimum yang disediakan.
10.3.1	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	netfw-logging-enabled	Pastikan firewall AWS Network Firewall telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika jenis logging tidak dikonfigurasi. Anda dapat menentukan jenis logging yang Anda ingin aturan untuk memeriksa.
10.3.2	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	cloudtrail-security-trail-enabled	Pastikan bahwa setidaknya ada satu AWS CloudTrail jejak yang ditentukan dengan praktik terbaik keamanan. Aturan ini SESUAI jika setidaknya ada satu jejak yang memenuhi semua hal berikut:

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.2	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	neptune-cluster-snapshot-public-dilarang	Pastikan snapshot cluster DB manual Amazon Neptunus tidak bersifat publik. Aturannya adalah NON_COMPLIANT jika ada snapshot cluster Neptunus yang ada dan yang baru bersifat publik.
10.3.2	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan brankas cadangan memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Aturannya adalah NON_COMPLIANT jika Brankas Cadangan tidak memiliki kebijakan berbasis sumber daya atau memiliki kebijakan tanpa pernyataan 'Deny' yang sesuai (pernyataan dengan cadangan: DeleteRecoveryPoint, cadangan:, dan cadangan: izin). UpdateRecoveryPointLifecycle PutBackupVaultAccessPolicy

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.2	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	emr-block-public-access	Pastikan akun dengan Amazon EMR telah mengaktifkan pengaturan akses publik yang diblokir. Aturannya adalah NON_COMPLIANT jika BlockPublicSecurityGroupRules salah, atau jika benar, port selain Port 22 terdaftar di. PermittedPublicSecurityGroupRuleRanges
10.3.2	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	s3- -blok access-point-public-access	Pastikan jalur akses Amazon S3 telah mengaktifkan pengaturan akses publik blok. Aturannya adalah NON_COMPLIANT jika pengaturan akses publik blok tidak diaktifkan untuk titik akses S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.2	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	s3- -blok account-level-public-access	Pastikan bahwa pengaturan blok akses publik yang diperlukan dikonfigurasi dari tingkat akun. Aturannya hanya NON_COMPLIANT jika bidang yang ditetapkan di bawah ini tidak cocok dengan bidang yang sesuai di item konfigurasi.
10.3.2	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	s3- bucket-mfa-delete-enabled	Pastikan MFA Delete diaktifkan di konfigurasi pembuatan versi bucket Amazon Simple Storage Service (Amazon S3). Aturannya adalah NON_COMPLIANT jika MFA Delete tidak diaktifkan.
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	aurora-resources-protected-by-rencana cadangan	Pastikan klaster Amazon Aurora DB dilindungi oleh paket cadangan. Aturannya adalah NON_COMPLIANT jika Cluster Database Amazon Relational Database Service (Amazon RDS) tidak dilindungi oleh paket cadangan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	db-instance-backup-enabled	Pastikan instans RDS DB memiliki cadangan yang diaktifkan. Secara opsional, aturan memeriksa periode retensi cadangan dan jendela cadangan.
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	dynamodb-in-backup-plan	Pastikan tabel Amazon DynamoDB ada di AWS Paket Cadangan. Aturannya adalah NON_COMPLIANT jika tabel Amazon DynamoDB tidak ada dalam paket Backup apa pun. AWS
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	dynamodb-resources-protected-by-rencana cadangan	Pastikan tabel Amazon DynamoDB dilindungi oleh paket cadangan. Aturannya adalah NON_COMPLIANT jika Tabel DynamoDB tidak dicakup oleh rencana cadangan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	ebs-in-backup-plan	Pastikan volume Amazon Elastic Block Store (Amazon EBS) ditambahk an dalam paket cadangan Backup. AWS Aturannya adalah NON_COMPL IANT jika volume Amazon EBS tidak disertakan dalam paket cadangan.
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	ebs-resources-prot ected-by-rencana cadangan	Pastikan volume Amazon Elastic Block Store (Amazon EBS) dilindungi oleh paket cadangan. Aturannya adalah NON_COMPL IANT jika volume Amazon EBS tidak dicakup oleh paket cadangan.
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	ec2- -rencana resources-protected-by-backup	Pastikan instans Amazon Elastic Compute Cloud (Amazon EC2) dilindungi oleh paket cadangan. Aturannya adalah NON_COMPLIANT EC2 jika instance Amazon tidak dicakup oleh paket cadangan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	efs-resources-protected-by-rencana cadangan	Pastikan sistem file Amazon Elastic File System (Amazon EFS) dilindungi oleh paket cadangan. Aturannya adalah NON_COMPLIANT jika Sistem File EFS tidak dicakup oleh rencana cadangan.
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	elasticache-redis-cluster-automatic-backup-periksa	Periksa apakah kluster Amazon ElastiCache Redis mengaktifkan cadangan otomatis. Aturannya adalah NON_COMPLIANT jika cluster SnapshotRetentionLimit for Redis kurang dari parameter . SnapshotRetentionPeriod Misalnya: Jika parameternya 15 maka aturannya tidak sesuai jika antara snapshotRetentionPeriod 0-15.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	fsx-resources-protected-by-rencana cadangan	Pastikan Sistem FSx File Amazon dilindungi oleh paket cadangan. Aturannya adalah NON_COMPLIANT jika Sistem FSx File Amazon tidak dicakup oleh paket cadangan.
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	neptune-cluster-backup-retention-periksa	Pastikan periode retensi klaster Amazon Neptunus DB diatur ke jumlah hari tertentu. Aturannya adalah NON_COMPLIANT jika periode retensi kurang dari nilai yang ditentukan oleh parameter.
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	rds-in-backup-plan	Pastikan database Amazon Relational Database Service (Amazon RDS) hadir dalam AWS paket Backup. Aturannya adalah NON_COMPLIANT jika database Amazon RDS tidak disertakan dalam paket Backup apa pun. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	redshift-backup-enabled	Pastikan snapshot otomatis Amazon Redshift diaktifkan untuk cluster. Aturannya adalah NON_COMPLIANT jika nilai untuk automatedSnapshotRetention Periode lebih besar dari MaxRetentionPeriod atau kurang dari MinRetentionPeriod atau nilainya 0.
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	s3- -rencana resources-protected-by-backup	Pastikan bucket Amazon Simple Storage Service (Amazon S3) dilindungi oleh paket cadangan. Aturannya adalah NON_COMPLIANT jika bucket Amazon S3 tidak tercakup oleh paket cadangan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	cloudtrail-security-trail-enabled	Pastikan bahwa setidaknya ada satu AWS CloudTrail jejak yang ditentukan dengan praktik terbaik keamanan. Aturan ini SESUAI jika setidakny a ada satu jejak yang memenuhi semua hal berikut:
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	db-instance-backup-enabled	Pastikan instans RDS DB memiliki cadangan yang diaktifkan. Secara opsional, aturan memeriksa periode retensi cadangan dan jendela cadangan.
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	dynamodb-pitr-enabled	Pastikan point-in-time pemulihan (PITR) diaktifkan untuk tabel Amazon DynamoDB. Aturannya adalah NON_COMPLIANT jika PITR tidak diaktifkan untuk tabel DynamoDB.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.4	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	s3- bucket-default-lock-enabled	Pastikan bucket S3 telah mengaktif kan kunci, secara default. Aturannya adalah NON_COMPLIANT jika kunci tidak diaktifkan.
10.3.4	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	s3- bucket-versioning-enabled	Pastikan pembuatan versi diaktifkan untuk bucket S3 Anda. Secara opsional, aturan memeriksa apakah penghapusan MFA diaktifkan untuk bucket S3 Anda.
10.3.4	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	cloudtrail-security-trail-enabled	Pastikan bahwa setidaknya ada satu AWS CloudTrail jejak yang ditentukan dengan praktik terbaik keamanan. Aturan ini SESUAI jika setidaknya ada satu jejak yang memenuhi semua hal berikut:

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
10.4.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	ec2- instance-detailed-monitoring-enabled	Pastikan pemantauan terperinci diaktifkan untuk EC2 instans. Aturannya adalah NON_COMPLIANT jika pemantauan terperinci tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	cloudwatch-alarm-resource-check	Pastikan bahwa jenis sumber daya memiliki CloudWatch alarm untuk metrik bernama. Untuk jenis sumber daya, Anda dapat menentukan volume EBS, EC2 instans, kluster Amazon RDS, atau bucket S3. Aturannya adalah COMPLIANT jika metrik bernama memiliki ID sumber daya dan CloudWatch alarm.
10.4.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	wafv2- rulegroup-logging-enabled	Pastikan pengumpulan metrik CloudWatch keamanan Amazon pada grup AWS WAFv2 aturan diaktifkan. Aturannya adalah NON_COMPLIANT jika '. VisibilityConfig CloudWatchMetricsEnabled'bidang disetel ke false.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	sns-topic-message-delivery-notifikasi-diaktifkan	Pastikan pencatatan Amazon Simple Notification Service (SNS) diaktifkan untuk status pengiriman pesan notifikasi yang dikirim ke topik untuk titik akhir. Aturannya adalah NON_COMPLIANT jika pemberitahuan status pengiriman untuk pesan tidak diaktifkan.
10.4.1.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
10.4.1.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	ec2- instance-detailed-monitoring-enabled	Pastikan pemantauan terperinci diaktifkan untuk EC2 instans. Aturannya adalah NON_COMPLIANT jika pemantauan terperinci tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.1.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.1.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.1.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.1.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	cloudwatch-alarm-resource-check	Pastikan bahwa jenis sumber daya memiliki CloudWatch alarm untuk metrik bernama. Untuk jenis sumber daya, Anda dapat menentukan volume EBS, EC2 instans, kluster Amazon RDS, atau bucket S3. Aturannya adalah COMPLIANT jika metrik bernama memiliki ID sumber daya dan CloudWatch alarm.
10.4.1.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	wafv2- rulegroup-logging-enabled	Pastikan pengumpulan metrik CloudWatch keamanan Amazon pada grup AWS WAFv2 aturan diaktifkan. Aturannya adalah NON_COMPLIANT jika '. VisibilityConfig CloudWatchMetricsEnabled'bidang disetel ke false.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.1.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	sns-topic-message-delivery-notifikasi-diaktifkan	Pastikan pencatatan Amazon Simple Notification Service (SNS) diaktifkan untuk status pengiriman pesan notifikasi yang dikirim ke topik untuk titik akhir. Aturannya adalah NON_COMPLIANT jika pemberitahuan status pengiriman untuk pesan tidak diaktifkan.
10.4.2	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
10.4.2	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	ec2- instance-detailed-monitoring-enabled	Pastikan pemantauan terperinci diaktifkan untuk EC2 instans. Aturannya adalah NON_COMPLIANT jika pemantauan terperinci tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.2	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.2	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.2	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.2	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	cloudwatch-alarm-resource-check	Pastikan bahwa jenis sumber daya memiliki CloudWatch alarm untuk metrik bernama. Untuk jenis sumber daya, Anda dapat menentukan volume EBS, EC2 instans, kluster Amazon RDS, atau bucket S3. Aturannya adalah COMPLIANT jika metrik bernama memiliki ID sumber daya dan CloudWatch alarm.
10.4.2	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	wafv2- rulegroup-logging-enabled	Pastikan pengumpulan metrik CloudWatch keamanan Amazon pada grup AWS WAFv2 aturan diaktifkan. Aturannya adalah NON_COMPLIANT jika '. VisibilityConfig CloudWatchMetricsEnabled'bidang disetel ke false.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.2	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	sns-topic-message-delivery-notifikasi-diaktifkan	Pastikan pencatatan Amazon Simple Notification Service (SNS) diaktifkan untuk status pengiriman pesan notifikasi yang dikirim ke topik untuk titik akhir. Aturannya adalah NON_COMPLIANT jika pemberitahuan status pengiriman untuk pesan tidak diaktifkan.
10.4.3	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.5.1	Riwayat log audit dipertahankan dan tersedia untuk analisis. (PCI-DSS-V4.0)	cloudtrail-security-trail-enabled	Pastikan bahwa setidaknya ada satu AWS CloudTrail jejak yang ditentukan dengan praktik terbaik keamanan. Aturan ini SESUAI jika setidakny a ada satu jejak yang memenuhi semua hal berikut:
10.5.1	Riwayat log audit dipertahankan dan tersedia untuk analisis. (PCI-DSS-V4.0)	ec2- volume-inuse-check	Pastikan volume EBS dilampirkan ke EC2 instance. Secara opsional memastika n bahwa volume EBS ditandai untuk dihapus ketika sebuah instance dihentikan.
10.5.1	Riwayat log audit dipertahankan dan tersedia untuk analisis. (PCI-DSS-V4.0)	ecr-private-lifecycle-policy-dikonfigurasi	Pastikan bahwa repositori Amazon Elastic Container Registry (ECR) pribadi memiliki setidaknya satu kebijakan siklus hidup yang dikonfigu rasi. Aturannya adalah NON_COMPL IANT jika tidak ada kebijakan siklus hidup yang dikonfigu rasi untuk repositori pribadi ECR.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.5.1	Riwayat log audit dipertahankan dan tersedia untuk analisis. (PCI-DSS-V4.0)	dynamodb-pitr-enabled	Pastikan point-in-time pemulihan (PITR) diaktifkan untuk tabel Amazon DynamoDB. Aturannya adalah NON_COMPLIANT jika PITR tidak diaktifkan untuk tabel DynamoDB.
10.5.1	Riwayat log audit dipertahankan dan tersedia untuk analisis. (PCI-DSS-V4.0)	cw-loggroup-retention-period-periksa	Pastikan periode CloudWatch LogGroup retensi Amazon diatur ke lebih dari 365 hari atau periode retensi tertentu. Aturannya adalah NON_COMPLIANT jika periode retensi kurang dari MinRetentionTime, jika ditentukan, atau 365 hari.
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	api-gwv2- access-logs-enabled	Pastikan tahap Amazon API Gateway V2 mengaktifkan pencatatan akses. Aturannya adalah NON_COMPLIANT jika 'accessLogSettings' tidak ada dalam konfigurasi Stage.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	s3- bucket-blacklisted-actions-prohibited	Pastikan kebijakan bucket Amazon Simple Storage Service (Amazon S3) tidak mengizinkan tindakan tingkat ember dan tingkat objek yang diblokir pada sumber daya dalam bucket untuk prinsipal dari akun lain. AWS Misalnya, aturan memeriksa bahwa kebijakan bucket Amazon S3 tidak mengizinkan AWS akun lain untuk melakukan tindakan s3: GetBucket * dan s3: DeleteObject pada objek apa pun di bucket. Aturannya adalah NON_COMPLIANT jika ada tindakan yang diblokir yang diizinkan oleh kebijakan bucket Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	s3- bucket-policy-not-more -permisif	Pastikan kebijakan bucket Amazon Simple Storage Service (S3) Anda tidak mengizinkan izin antar akun selain kebijakan bucket Amazon S3 kontrol yang Anda berikan.
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	neptune-cluster-cloudwatch-log-ekspor diaktifkan	Pastikan klaster CloudWatch Amazon Neptunus mengaktifkan ekspor log untuk log audit. Aturannya adalah NON_COMPLIANT jika klaster Neptunus tidak mengaktifkan ekspor log untuk log audit. CloudWatch
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	ec2- instance-detailed-monitoring-enabled	Pastikan pemantauan terperinci diaktifkan untuk EC2 instans. Aturannya adalah NON_COMPLIANT jika pemantauan terperinci tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	ecs-task-definition-log-konfigurasi	Pastikan bahwa LogConfiguration diatur pada Definisi Tugas ECS aktif. Aturan ini NON_COMPLIANT jika ECSTask Definisi aktif tidak memiliki sumber daya LogConfiguration yang ditentukan atau nilai untuk LogConfiguration adalah null dalam setidaknya satu definisi kontainer.
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	cloudwatch-alarm-resource-check	Pastikan bahwa jenis sumber daya memiliki CloudWatch alarm untuk metrik bernama. Untuk jenis sumber daya, Anda dapat menentukan volume EBS, EC2 instans, kluster Amazon RDS, atau bucket S3. Aturannya adalah COMPLIANT jika metrik bernama memiliki ID sumber daya dan CloudWatch alarm.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	cloudtrail-diaktifkan	Catatan: Untuk aturan ini, pengidentifikasi aturan (CLOUD_TRAIL_ENABLED) dan nama aturan (cloudtrail-enabled) berbeda. Pastikan AWS CloudTrail jejak diaktifkan di AWS akun Anda. Aturannya adalah NON_COMPLIANT jika jejak tidak diaktifkan. Secara opsional, aturan memeriksa bucket S3 tertentu, topik Amazon Simple Notification Service (Amazon SNS), dan grup log. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	multi-region-cloudtrail-enabled	Catatan: untuk aturan ini, pengidentifikasi aturan (MULTI_REGION_CLOUD_TRAIL_ENABLED) dan nama aturan () berbeda. multi-region-cloudtrail-enabled Pastikan setidaknya ada satu multi-wilayah AWS CloudTrail. Aturannya adalah NON_COMPLIANT jika jejak tidak cocok dengan parameter input. Aturannya adalah NON_COMPLIANT jika ExcludeManagementEventSources bidang tidak kosong atau jika AWS CloudTrail dikonfigurasi untuk mengecualikan peristiwa manajemen seperti peristiwa AWS KMS atau peristiwa API Data Amazon RDS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	appsync-logging-enabled	Pastikan bahwa AWS AppSync API telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan, atau 'fieldLogLevel' bukan ERROR atau SEMUA.
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	mq-cloudwatch-audit-logging-diaktifkan	Pastikan pialang Amazon MQ mengaktifkan pencatatan CloudWatch audit Amazon. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	mq-cloudwatch-audit-log-diaktifkan	Pastikan bahwa broker Amazon MQ mengaktifkan pencatatan CloudWatch audit. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	eks-cluster-logging-enabled	Pastikan klaster Amazon Elastic Kubernetes Service (Amazon EKS) dikonfigurasi dengan logging diaktifkan. Aturannya adalah NON_COMPLIANT jika logging untuk klaster Amazon EKS tidak diaktifkan untuk semua jenis log.
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	elastic-beanstalk-logs-to-jam tangan awan	Pastikan lingkungan AWS Elastic Beanstalk dikonfigurasi untuk mengirim log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika nilai `StreamLogs` salah.
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	wafv2- rulegroup-logging-enabled	Pastikan pengumpulan metrik CloudWatch keamanan Amazon pada grup AWS WAFv2 aturan diaktifkan. Aturannya adalah NON_COMPLIANT jika '. VisibilityConfig CloudWatchMetricsEnabled'bidang disetel ke false.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	sns-topic-message-delivery-notifikasi-diaktifkan	Pastikan pencatatan Amazon Simple Notification Service (SNS) diaktifkan untuk status pengiriman pesan notifikasi yang dikirim ke topik untuk titik akhir. Aturannya adalah NON_COMPLIANT jika pemberitahuan status pengiriman untuk pesan tidak diaktifkan.
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	step-functions-state-machine-logging-diaktifkan	Pastikan bahwa mesin AWS Step Functions telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika mesin status tidak mengaktifkan logging atau konfigurasi logging tidak pada tingkat minimum yang disediakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	netfw-logging-enabled	Pastikan firewall AWS Network Firewall telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika jenis logging tidak dikonfigurasi. Anda dapat menentukan jenis logging yang Anda ingin aturan untuk memeriksa.
10.7.1	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
10.7.1	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	ec2- instance-detailed-monitoring-enabled	Pastikan pemantauan terperinci diaktifkan untuk EC2 instans. Aturannya adalah NON_COMPLIANT jika pemantauan terperinci tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.7.1	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.7.1	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.7.1	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.7.1	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	cloudwatch-alarm-resource-check	Pastikan bahwa jenis sumber daya memiliki CloudWatch alarm untuk metrik bernama. Untuk jenis sumber daya, Anda dapat menentukan volume EBS, EC2 instans, kluster Amazon RDS, atau bucket S3. Aturannya adalah COMPLIANT jika metrik bernama memiliki ID sumber daya dan CloudWatch alarm.
10.7.1	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	wafv2- rulegroup-logging-enabled	Pastikan pengumpulan metrik CloudWatch keamanan Amazon pada grup AWS WAFv2 aturan diaktifkan. Aturannya adalah NON_COMPLIANT jika '. VisibilityConfig CloudWatchMetricsEnabled'bidang disetel ke false.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.7.1	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	sns-topic-message-delivery-notifikasi-diaktifkan	Pastikan pencatatan Amazon Simple Notification Service (SNS) diaktifkan untuk status pengiriman pesan notifikasi yang dikirim ke topik untuk titik akhir. Aturannya adalah NON_COMPLIANT jika pemberitahuan status pengiriman untuk pesan tidak diaktifkan.
10.7.2	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
10.7.2	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	ec2- instance-detailed-monitoring-enabled	Pastikan pemantauan terperinci diaktifkan untuk EC2 instans. Aturannya adalah NON_COMPLIANT jika pemantauan terperinci tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.7.2	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.7.2	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.7.2	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.7.2	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	cloudwatch-alarm-resource-check	Pastikan bahwa jenis sumber daya memiliki CloudWatch alarm untuk metrik bernama. Untuk jenis sumber daya, Anda dapat menentukan volume EBS, EC2 instans, kluster Amazon RDS, atau bucket S3. Aturannya adalah COMPLIANT jika metrik bernama memiliki ID sumber daya dan CloudWatch alarm.
10.7.2	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	wafv2- rulegroup-logging-enabled	Pastikan pengumpulan metrik CloudWatch keamanan Amazon pada grup AWS WAFv2 aturan diaktifkan. Aturannya adalah NON_COMPLIANT jika '. VisibilityConfig CloudWatchMetricsEnabled'bidang disetel ke false.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.7.2	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	sns-topic-message-delivery-notifikasi-diaktifkan	Pastikan pencatatan Amazon Simple Notification Service (SNS) diaktifkan untuk status pengiriman pesan notifikasi yang dikirim ke topik untuk titik akhir. Aturannya adalah NON_COMPLIANT jika pemberitahuan status pengiriman untuk pesan tidak diaktifkan.
11.5.2	Intrusi jaringan dan perubahan file yang tidak terduga terdeteksi dan ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.5.2	Intrusi jaringan dan perubahan file yang tidak terduga terdeteksi dan ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.
11.5.2	Intrusi jaringan dan perubahan file yang tidak terduga terdeteksi dan ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-settings-check	Pastikan CloudWatch alarm dengan nama metrik yang diberikan memiliki pengaturan yang ditentukan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.5.2	Intrusi jaringan dan perubahan file yang tidak terduga terdeteksi dan ditanggapi. (PCI-DSS-V4.0)	sns-topic-message-delivery-notifikasi-diaktifkan	Pastikan pencatatan Amazon Simple Notification Service (SNS) diaktifkan untuk status pengiriman pesan notifikasi yang dikirim ke topik untuk titik akhir. Aturannya adalah NON_COMPLIANT jika pemberitahuan status pengiriman untuk pesan tidak diaktifkan.
11.6.1	Perubahan yang tidak sah pada halaman pembayaran terdeteksi dan ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.6.1	Perubahan yang tidak sah pada halaman pembayaran terdeteksi dan ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.
11.6.1	Perubahan yang tidak sah pada halaman pembayaran terdeteksi dan ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-settings-check	Pastikan CloudWatch alarm dengan nama metrik yang diberikan memiliki pengaturan yang ditentukan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.6.1	Perubahan yang tidak sah pada halaman pembayaran terdeteksi dan ditanggapi. (PCI-DSS-V4.0)	sns-topic-message-delivery-notifikasi-diaktifkan	Pastikan pencatatan Amazon Simple Notification Service (SNS) diaktifkan untuk status pengiriman pesan notifikasi yang dikirim ke topik untuk titik akhir. Aturannya adalah NON_COMPLIANT jika pemberitahuan status pengiriman untuk pesan tidak diaktifkan.
12.10.5	Insiden keamanan yang dicurigai dan dikonfirmasi yang dapat berdampak pada CDE segera ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.10.5	Insiden keamanan yang dicurigai dan dikonfirmasi yang dapat berdampak pada CDE segera ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.
12.10.5	Insiden keamanan yang dicurigai dan dikonfirmasi yang dapat berdampak pada CDE segera ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-settings-check	Pastikan CloudWatch alarm dengan nama metrik yang diberikan memiliki pengaturan yang ditentukan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.10.5	Insiden keamanan yang dicurigai dan dikonfirmasi yang dapat berdampak pada CDE segera ditanggapi. (PCI-DSS-V4.0)	sns-topic-message-delivery-notifikasi-diaktifkan	Pastikan pencatatan Amazon Simple Notification Service (SNS) diaktifkan untuk status pengiriman pesan notifikasi yang dikirim ke topik untuk titik akhir. Aturannya adalah NON_COMPLIANT jika pemberitahuan status pengiriman untuk pesan tidak diaktifkan.
12.4.2.1	Kepatuhan PCI DSS dikelola. (PCI-DSS-V4.0)	service-catalog-shared-within-organisasi	Pastikan bahwa AWS Service Catalog membagikan portofolio ke organisasi (kumpulan AWS akun yang diperlakukan sebagai satu unit) saat integrasi diaktifkan dengan Organizations AWS . Aturannya adalah NON_COMPLIANT jika nilai `Type` dari sebuah share adalah `ACCOUNT`.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.5	Komponen sistem dikonfigurasi dan dikelola dengan aman. (PCI-DSS-V4.0)	transfer-family-server-no-ftp	Pastikan server yang dibuat dengan AWS Transfer Family tidak menggunakan FTP untuk koneksi endpoint. Aturannya adalah NON_COMPLIANT jika protokol server untuk koneksi endpoint diaktifkan FTP.
2.2.7	Komponen sistem dikonfigurasi dan dikelola dengan aman. (PCI-DSS-V4.0)	dms-redis-tls-enabled	Pastikan titik akhir AWS Database Migration Service (AWS DMS) untuk penyimpanan data Redis diaktifkan untuk TLS/SSL encryption of data communicated with other endpoints. The rule is NON_COMPLIANT if TLS/SSL enkripsi tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.7	Komponen sistem dikonfigurasi dan dikelola dengan aman. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.7	Komponen sistem dikonfigurasi dan dikelola dengan aman. (PCI-DSS-V4.0)	msk-in-cluster-node-membutuhkan-tls	Pastikan bahwa klaster MSK Amazon memberlakukan enkripsi dalam perjalanan menggunakan HTTPS (TLS) dengan node broker klaster. Aturannya adalah NON_COMPLIANT jika komunikasi teks biasa diaktifkan untuk koneksi node broker in-cluster.
2.2.7	Komponen sistem dikonfigurasi dan dikelola dengan aman. (PCI-DSS-V4.0)	dms-endpoint-ssl-configured	Pastikan titik akhir AWS Database Migration Service (AWS DMS) dikonfigurasi dengan koneksi SSL. Aturannya adalah NON_COMPLIANT jika AWS DMS tidak memiliki koneksi SSL yang dikonfigurasi.
3.2.1	Penyimpanan data akun dijaga seminimal mungkin. (PCI-DSS-V4.0)	ec2- volume-inuse-check	Pastikan volume EBS dilampirkan ke EC2 instance. Secara opsional memastikan bahwa volume EBS ditandai untuk dihapus ketika sebuah instance dihentikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.2.1	Penyimpanan data akun dijaga seminimal mungkin. (PCI-DSS-V4.0)	ecr-private-lifecycle-policy-dikonfigurasi	Pastikan bahwa repositori Amazon Elastic Container Registry (ECR) pribadi memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi. Aturannya adalah NON_COMPLIANT jika tidak ada kebijakan siklus hidup yang dikonfigurasi untuk repositori pribadi ECR.
3.2.1	Penyimpanan data akun dijaga seminimal mungkin. (PCI-DSS-V4.0)	dynamodb-pitr-enabled	Pastikan point-in-time pemulihan (PITR) diaktifkan untuk tabel Amazon DynamoDB. Aturannya adalah NON_COMPLIANT jika PITR tidak diaktifkan untuk tabel DynamoDB.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.2.1	Penyimpanan data akun dijaga seminimal mungkin. (PCI-DSS-V4.0)	cw-loggroup-retention-period-periksa	Pastikan periode CloudWatch LogGroup retensi Amazon diatur ke lebih dari 365 hari atau periode retensi tertentu. Aturannya adalah NON_COMPLIANT jika periode retensi kurang dari MinRetentionTime, jika ditentukan, atau 365 hari.
3.3.1.1	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	ec2- volume-inuse-check	Pastikan volume EBS dilampirkan ke EC2 instance. Secara opsional memastikan bahwa volume EBS ditandai untuk dihapus ketika sebuah instance dihentikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1.1	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	ecr-private-lifecycle-policy-dikonfigurasi	Pastikan bahwa repositori Amazon Elastic Container Registry (ECR) pribadi memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi. Aturannya adalah NON_COMPLIANT jika tidak ada kebijakan siklus hidup yang dikonfigurasi untuk repositori pribadi ECR.
3.3.1.1	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	dynamodb-pitr-enabled	Pastikan point-in-time pemulihan (PITR) diaktifkan untuk tabel Amazon DynamoDB. Aturannya adalah NON_COMPLIANT jika PITR tidak diaktifkan untuk tabel DynamoDB.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1.1	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	cw-loggroup-retention-period-periksa	Pastikan periode CloudWatch LogGroup retensi Amazon diatur ke lebih dari 365 hari atau periode retensi tertentu. Aturannya adalah NON_COMPLIANT jika periode retensi kurang dari MinRetentionTime, jika ditentukan, atau 365 hari.
3.3.1.3	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	ec2- volume-inuse-check	Pastikan volume EBS dilampirkan ke EC2 instance. Secara opsional memastikan bahwa volume EBS ditandai untuk dihapus ketika sebuah instance dihentikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1.3	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	ecr-private-lifecycle-policy-dikonfigurasi	Pastikan bahwa repositori Amazon Elastic Container Registry (ECR) pribadi memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi. Aturannya adalah NON_COMPLIANT jika tidak ada kebijakan siklus hidup yang dikonfigurasi untuk repositori pribadi ECR.
3.3.1.3	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	dynamodb-pitr-enabled	Pastikan point-in-time pemulihan (PITR) diaktifkan untuk tabel Amazon DynamoDB. Aturannya adalah NON_COMPLIANT jika PITR tidak diaktifkan untuk tabel DynamoDB.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1.3	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	cw-loggroup-retention-period-periksa	Pastikan periode CloudWatch LogGroup retensi Amazon diatur ke lebih dari 365 hari atau periode retensi tertentu. Aturannya adalah NON_COMPLIANT jika periode retensi kurang dari MinRetentionTime, jika ditentukan, atau 365 hari.
3.3.2	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	ec2- volume-inuse-check	Pastikan volume EBS dilampirkan ke EC2 instance. Secara opsional memastikan bahwa volume EBS ditandai untuk dihapus ketika sebuah instance dihentikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.2	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	ecr-private-lifecycle-policy-dikonfigurasi	Pastikan bahwa repositori Amazon Elastic Container Registry (ECR) pribadi memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi. Aturannya adalah NON_COMPLIANT jika tidak ada kebijakan siklus hidup yang dikonfigurasi untuk repositori pribadi ECR.
3.3.2	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	dynamodb-pitr-enabled	Pastikan point-in-time pemulihan (PITR) diaktifkan untuk tabel Amazon DynamoDB. Aturannya adalah NON_COMPLIANT jika PITR tidak diaktifkan untuk tabel DynamoDB.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.2	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	cw-loggroup-retention-period-periksa	Pastikan periode CloudWatch LogGroup retensi Amazon diatur ke lebih dari 365 hari atau periode retensi tertentu. Aturannya adalah NON_COMPLIANT jika periode retensi kurang dari MinRetentionTime, jika ditentukan, atau 365 hari.
3.3.3	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	ec2- volume-inuse-check	Pastikan volume EBS dilampirkan ke EC2 instance. Secara opsional memastikan bahwa volume EBS ditandai untuk dihapus ketika sebuah instance dihentikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.3	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	ecr-private-lifecycle-policy-dikonfigurasi	Pastikan bahwa repositori Amazon Elastic Container Registry (ECR) pribadi memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi. Aturannya adalah NON_COMPLIANT jika tidak ada kebijakan siklus hidup yang dikonfigurasi untuk repositori pribadi ECR.
3.3.3	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	dynamodb-pitr-enabled	Pastikan point-in-time pemulihan (PITR) diaktifkan untuk tabel Amazon DynamoDB. Aturannya adalah NON_COMPLIANT jika PITR tidak diaktifkan untuk tabel DynamoDB.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.3	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	cw-loggroup-retention-period-periksa	Pastikan periode CloudWatch LogGroup retensi Amazon diatur ke lebih dari 365 hari atau periode retensi tertentu. Aturannya adalah NON_COMPLIANT jika periode retensi kurang dari MinRetentionTime, jika ditentukan, atau 365 hari.
3.5.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	athena-workgroup-encrypted-at-istirahat	Pastikan bahwa workgroup Amazon Athena dienkripsi saat istirahat. Aturannya adalah NON_COMPLIANT jika enkripsi data saat istirahat tidak diaktifkan untuk workgroup Athena.
3.5.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	neptune-cluster-snapshot-encrypted	Pastikan bahwa kluster Amazon Neptunus DB memiliki snapshot yang dienkripsi. Aturannya adalah NON_COMPLIANT jika cluster Neptunus tidak memiliki snapshot yang dienkripsi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	redshift-cluster-kms-enabled	Pastikan bahwa klaster Amazon Redshift menggunakan AWS kunci Key Management Service (AWS KMS) yang ditentukan untuk enkripsi. Aturannya adalah COMPLIANT jika enkripsi diaktifkan dan cluster dienkripsi dengan kunci yang disediakan dalam parameter. kmsKeyArn Aturannya adalah NON_COMPLIANT jika cluster tidak dienkripsi atau dienkripsi dengan kunci lain.
3.5.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	codebuild-project-s3-log-terenkripsi	Pastikan AWS CodeBuild proyek yang dikonfigurasi dengan Amazon S3 Logs mengaktifkan enkripsi untuk lognya. Aturannya adalah NON_COMPLIANT jika 'EncryptionDisabled' disetel ke 'true' dalam S3 proyek. LogsConfig CodeBuild

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	eks-secrets-encrypted	Pastikan bahwa klaster Amazon Elastic Kubernete s Service dikonfigu rasi agar rahasia Kubernetes dienkrips i menggunakan kunci Key Management Service (KMS). AWS
3.5.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	api-gw-cache-enabl ed-dan-dienkripsi	Pastikan bahwa semua metode dalam tahapan Amazon API Gateway telah mengaktifkan cache dan cache dienkrips i. Aturannya adalah NON_COMPLIANT jika metode apa pun dalam tahap Amazon API Gateway tidak dikonfigurasi ke cache atau cache tidak dienkripsi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	dynamodb-table-encrypted-kms	Pastikan tabel Amazon DynamoDB dienkripsi AWS dengan Key Management Service (KMS). Aturannya adalah NON_COMPLIANT jika tabel Amazon DynamoDB tidak dienkripsi dengan KMS. AWS Aturannya juga NON_COMPLIANT jika kunci AWS KMS terenkripsi tidak ada dalam parameter input. kmsKeyArns
3.5.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	codebuild-project-envvar-awscred-periksa	Pastikan bahwa proyek TIDAK berisi variabel lingkungan AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY. Aturannya adalah NON_COMPLIANT ketika variabel lingkungan proyek berisi kredensyal teks biasa.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	eks-cluster-secrets-encrypted	Pastikan bahwa klaster Amazon EKS tidak dikonfigurasi agar rahasia Kubernetes dienkripsi menggunakan KMS. AWS Aturannya adalah NON_COMPLIANT jika kluster EKS tidak memiliki sumber daya EncryptionConfig atau jika EncryptionConfig tidak menyebutkan rahasia sebagai sumber daya.
3.5.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	kinesis-stream-encrypted	Pastikan aliran Amazon Kinesis dienkripsi saat istirahat dengan enkripsi sisi server. Aturannya adalah NON_COMPLIANT untuk aliran Kinesis jika " StreamEncryption tidak ada.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	neptune-cluster-encrypted	Pastikan enkripsi penyimpanan diaktifkan untuk kluster Amazon Neptunus DB Anda. Aturannya adalah NON_COMPLIANT jika enkripsi penyimpanan tidak diaktifkan.
3.5.1.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	acm-pca-root-ca-dinonaktifkan	Pastikan AWS Private Certificate Authority (AWS Private CA) memiliki CA root yang dinonaktifkan. Aturannya adalah NON_COMPLIANT untuk root CAs dengan status yang tidak DINONAKTIFKAN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.1.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.
3.5.1.3	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	acm-pca-root-ca-dinonaktifkan	Pastikan AWS Private Certificate Authority (AWS Private CA) memiliki CA root yang dinonaktifkan. Aturannya adalah NON_COMPLIANT untuk root CAs dengan status yang tidak DINONAKTIFKAN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.1.3	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	neptune-cluster-snapshot-public-dilarang	Pastikan snapshot cluster DB manual Amazon Neptunus tidak bersifat publik. Aturannya adalah NON_COMPLIANT jika ada snapshot cluster Neptunus yang ada dan yang baru bersifat publik.
3.5.1.3	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan brankas cadangan memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Aturannya adalah NON_COMPLIANT jika Brankas Cadangan tidak memiliki kebijakan berbasis sumber daya atau memiliki kebijakan tanpa pernyataan 'Deny' yang sesuai (pernyataan dengan cadangan: DeleteRecoveryPoint, cadangan:, dan cadangan: izin). UpdateRecoveryPointLifecycle PutBackupVaultAccessPolicy

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.1.3	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.1.3	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	emr-block-public-access	Pastikan akun dengan Amazon EMR telah mengaktifkan pengaturan akses publik yang diblokir. Aturannya adalah NON_COMPLIANT jika BlockPublicSecurityGroupRules salah, atau jika benar, port selain Port 22 terdaftar di. PermittedPublicSecurityGroupRuleRanges
3.5.1.3	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	s3- -blok access-point-public-access	Pastikan jalur akses Amazon S3 telah mengaktifkan pengaturan akses publik blok. Aturannya adalah NON_COMPLIANT jika pengaturan akses publik blok tidak diaktifkan untuk titik akses S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.1.3	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	s3- -blok account-level-public-access	Pastikan bahwa pengaturan blok akses publik yang diperlukan dikonfigurasi dari tingkat akun. Aturannya hanya NON_COMPLIANT jika bidang yang ditetapkan di bawah ini tidak cocok dengan bidang yang sesuai di item konfigurasi.
3.5.1.3	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	s3- bucket-mfa-delete-enabled	Pastikan MFA Delete diaktifkan di konfigurasi pembuatan versi bucket Amazon Simple Storage Service (Amazon S3). Aturannya adalah NON_COMPLIANT jika MFA Delete tidak diaktifkan.
3.6.1	Kunci kriptografi yang digunakan untuk melindungi data akun yang disimpan diamankan. (PCI-DSS-V4.0)	acm-pca-root-ca-dinonaktifkan	Pastikan AWS Private Certificate Authority (AWS Private CA) memiliki CA root yang dinonaktifkan. Aturannya adalah NON_COMPLIANT untuk root CAs dengan status yang tidak DINONAKTIFKAN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.1	Kunci kriptografi yang digunakan untuk melindungi data akun yang disimpan diamankan. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.
3.6.1.2	Kunci kriptografi yang digunakan untuk melindungi data akun yang disimpan diamankan. (PCI-DSS-V4.0)	acm-pca-root-ca-dinonaktifkan	Pastikan AWS Private Certificate Authority (AWS Private CA) memiliki CA root yang dinonaktifkan. Aturannya adalah NON_COMPLIANT untuk root CAs dengan status yang tidak DINONAKTIFKAN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.1.2	Kunci kriptografi yang digunakan untuk melindungi data akun yang disimpan diamankan. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.
3.6.1.3	Kunci kriptografi yang digunakan untuk melindungi data akun yang disimpan diamankan. (PCI-DSS-V4.0)	acm-pca-root-ca-dinonaktifkan	Pastikan AWS Private Certificate Authority (AWS Private CA) memiliki CA root yang dinonaktifkan. Aturannya adalah NON_COMPLIANT untuk root CAs dengan status yang tidak DINONAKTIFKAN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.1.3	Kunci kriptografi yang digunakan untuk melindungi data akun yang disimpan diamankan. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.
3.6.1.4	Kunci kriptografi yang digunakan untuk melindungi data akun yang disimpan diamankan. (PCI-DSS-V4.0)	acm-pca-root-ca-dinonaktifkan	Pastikan AWS Private Certificate Authority (AWS Private CA) memiliki CA root yang dinonaktifkan. Aturannya adalah NON_COMPLIANT untuk root CAs dengan status yang tidak DINONAKTIFKAN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.1.4	Kunci kriptografi yang digunakan untuk melindungi data akun yang disimpan diamankan. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.
3.7.1	Di mana kriptografi digunakan untuk melindungi data akun yang tersimpan, proses dan prosedur manajemen kunci yang mencakup semua aspek siklus hidup utama didefinisikan dan diimplementasikan. (PCI-DSS-V4.0)	acm-certificate-rsa-check	Pastikan sertifikat RSA yang dikelola oleh AWS Certificate Manager (ACM) memiliki panjang kunci minimal '2048' bit. Aturannya adalah NON_COMPLIANT jika panjang kunci minimum kurang dari 2048 bit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.7.1	Di mana kriptografi digunakan untuk melindungi data akun yang tersimpan, proses dan prosedur manajemen kunci yang mencakup semua aspek siklus hidup utama didefinisikan dan diimplementasikan. (PCI-DSS-V4.0)	acm-pca-root-ca-dinonaktifkan	Pastikan AWS Private Certificate Authority (AWS Private CA) memiliki CA root yang dinonaktifkan. Aturannya adalah NON_COMPLIANT untuk root CAs dengan status yang tidak DINONAKTIFKAN.
3.7.1	Di mana kriptografi digunakan untuk melindungi data akun yang tersimpan, proses dan prosedur manajemen kunci yang mencakup semua aspek siklus hidup utama didefinisikan dan diimplementasikan. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.7.2	Di mana kriptografi digunakan untuk melindungi data akun yang tersimpan, proses dan prosedur manajemen kunci yang mencakup semua aspek siklus hidup utama didefinisikan dan diimplementasikan. (PCI-DSS-V4.0)	acm-pca-root-ca-dinonaktifkan	Pastikan AWS Private Certificate Authority (AWS Private CA) memiliki CA root yang dinonaktifkan. Aturannya adalah NON_COMPLIANT untuk root CAs dengan status yang tidak DINONAKTIFKAN.
3.7.2	Di mana kriptografi digunakan untuk melindungi data akun yang tersimpan, proses dan prosedur manajemen kunci yang mencakup semua aspek siklus hidup utama didefinisikan dan diimplementasikan. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.7.4	Di mana kriptografi digunakan untuk melindungi data akun yang tersimpan, proses dan prosedur manajemen kunci yang mencakup semua aspek siklus hidup utama didefinisikan dan diimplementasikan. (PCI-DSS-V4.0)	acm-pca-root-ca-dinonaktifkan	Pastikan AWS Private Certificate Authority (AWS Private CA) memiliki CA root yang dinonaktifkan. Aturannya adalah NON_COMPLIANT untuk root CAs dengan status yang tidak DINONAKTIFKAN.
3.7.4	Di mana kriptografi digunakan untuk melindungi data akun yang tersimpan, proses dan prosedur manajemen kunci yang mencakup semua aspek siklus hidup utama didefinisikan dan diimplementasikan. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.7.6	Di mana kriptografi digunakan untuk melindungi data akun yang tersimpan, proses dan prosedur manajemen kunci yang mencakup semua aspek siklus hidup utama didefinisikan dan diimplementasikan. (PCI-DSS-V4.0)	acm-pca-root-ca-dinonaktifkan	Pastikan AWS Private Certificate Authority (AWS Private CA) memiliki CA root yang dinonaktifkan. Aturannya adalah NON_COMPLIANT untuk root CAs dengan status yang tidak DINONAKTIFKAN.
3.7.6	Di mana kriptografi digunakan untuk melindungi data akun yang tersimpan, proses dan prosedur manajemen kunci yang mencakup semua aspek siklus hidup utama didefinisikan dan diimplementasikan. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.7.7	Di mana kriptografi digunakan untuk melindungi data akun yang tersimpan, proses dan prosedur manajemen kunci yang mencakup semua aspek siklus hidup utama didefinisikan dan diimplementasikan. (PCI-DSS-V4.0)	acm-pca-root-ca-dinonaktifkan	Pastikan AWS Private Certificate Authority (AWS Private CA) memiliki CA root yang dinonaktifkan. Aturannya adalah NON_COMPLIANT untuk root CAs dengan status yang tidak DINONAKTIFKAN.
3.7.7	Di mana kriptografi digunakan untuk melindungi data akun yang tersimpan, proses dan prosedur manajemen kunci yang mencakup semua aspek siklus hidup utama didefinisikan dan diimplementasikan. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.2.1	PAN dilindungi dengan kriptografi yang kuat selama transmisi. (PCI-DSS-V4.0)	dms-redis-tls-enabled	Pastikan titik akhir AWS Database Migration Service (AWS DMS) untuk penyimpanan data Redis diaktifkan untuk TLS/SSL encryption of data communicated with other endpoints. The rule is NON_COMPLIANT if TLS/SSL enkripsi tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.2.1	PAN dilindungi dengan kriptografi yang kuat selama transmisi. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.2.1	PAN dilindungi dengan kriptografi yang kuat selama transmisi. (PCI-DSS-V4.0)	msk-in-cluster-node-membutuhkan-tls	Pastikan bahwa klaster MSK Amazon memberlakukan enkripsi dalam perjalanan menggunakan HTTPS (TLS) dengan node broker klaster. Aturannya adalah NON_COMPLIANT jika komunikasi teks biasa diaktifkan untuk koneksi node broker in-cluster.
4.2.1	PAN dilindungi dengan kriptografi yang kuat selama transmisi. (PCI-DSS-V4.0)	dms-endpoint-ssl-configured	Pastikan titik akhir AWS Database Migration Service (AWS DMS) dikonfigurasi dengan koneksi SSL. Aturannya adalah NON_COMPLIANT jika AWS DMS tidak memiliki koneksi SSL yang dikonfigurasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.2.1.1	PAN dilindungi dengan kriptografi yang kuat selama transmisi. (PCI-DSS-V4.0)	acm-pca-root-ca-dinonaktifkan	Pastikan AWS Private Certificate Authority (AWS Private CA) memiliki CA root yang dinonaktifkan. Aturannya adalah NON_COMPLIANT untuk root CAs dengan status yang tidak DINONAKTIFKAN.
4.2.1.1	PAN dilindungi dengan kriptografi yang kuat selama transmisi. (PCI-DSS-V4.0)	cloudfront-custom-ssl-certificate	Pastikan sertifikat yang terkait dengan CloudFront distribusi Amazon bukan sertifikat SSL default. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi menggunakan sertifikat SSL default.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.2.1.1	PAN dilindungi dengan kriptografi yang kuat selama transmisi. (PCI-DSS-V4.0)	dms-redis-tls-enabled	Pastikan titik akhir AWS Database Migration Service (AWS DMS) untuk penyimpanan data Redis diaktifkan untuk TLS/SSL encryption of data communicated with other endpoints. The rule is NON_COMPLIANT if TLS/SSL enkripsi tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.2.1.1	PAN dilindungi dengan kriptografi yang kuat selama transmisi. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancers . Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.2.1.1	PAN dilindungi dengan kriptografi yang kuat selama transmisi. (PCI-DSS-V4.0)	msk-in-cluster-node-membutuhkan-tls	Pastikan bahwa klaster MSK Amazon memberlakukan enkripsi dalam perjalanan menggunakan HTTPS (TLS) dengan node broker klaster. Aturannya adalah NON_COMPLIANT jika komunikasi teks biasa diaktifkan untuk koneksi node broker in-cluster.
4.2.1.1	PAN dilindungi dengan kriptografi yang kuat selama transmisi. (PCI-DSS-V4.0)	dms-endpoint-ssl-configured	Pastikan titik akhir AWS Database Migration Service (AWS DMS) dikonfigurasi dengan koneksi SSL. Aturannya adalah NON_COMPLIANT jika AWS DMS tidak memiliki koneksi SSL yang dikonfigurasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	api-gwv2- access-logs-enabled	Pastikan tahap Amazon API Gateway V2 mengaktifkan pencatatan akses. Aturannya adalah NON_COMPLIANT jika 'accessLogSettings' tidak ada dalam konfigurasi Stage.
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	cloudtrail-security-trail-enabled	Pastikan bahwa setidaknya ada satu AWS CloudTrail jejak yang ditentukan dengan praktik terbaik keamanan. Aturan ini SESUAI jika setidaknya ada satu jejak yang memenuhi semua hal berikut:

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	neptune-cluster-cloudwatch-log-ekspor diaktifkan	Pastikan klaster CloudWatch Amazon Neptunus mengaktifkan ekspor log untuk log audit. Aturannya adalah NON_COMPLIANT jika klaster Neptunus tidak mengaktifkan ekspor log untuk log audit. CloudWatch
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	ecs-task-definition-log-konfigurasi	Pastikan bahwa LogConfiguration diatur pada Definisi Tugas ECS aktif. Aturan ini NON_COMPLIANT jika ECSTask Definisi aktif tidak memiliki sumber daya LogConfiguration yang ditentukan atau nilai untuk LogConfiguration adalah null dalam setidaknya satu definisi kontainer.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	cloudtrail-diaktifkan	Catatan: Untuk aturan ini, pengidentifikasi aturan (CLOUD_TRAIL_ENABLED) dan nama aturan (cloudtrail-enabled) berbeda. Pastikan AWS CloudTrail jejak diaktifkan di AWS akun Anda. Aturannya adalah NON_COMPLIANT jika jejak tidak diaktifkan. Secara opsional, aturan memeriksa bucket S3 tertentu, topik Amazon Simple Notification Service (Amazon SNS), dan grup log. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	multi-region-cloudtrail-enabled	Catatan: untuk aturan ini, pengidentifikasi aturan (MULTI_REGION_CLOUD_TRAIL_ENABLED) dan nama aturan () berbeda. multi-region-cloudtrail-enabled Pastikan setidaknya ada satu multi-wilayah AWS CloudTrail. Aturannya adalah NON_COMPLIANT jika jejak tidak cocok dengan parameter input. Aturannya adalah NON_COMPLIANT jika ExcludeManagementEventSources bidang tidak kosong atau jika AWS CloudTrail dikonfigurasi untuk mengecualikan peristiwa manajemen seperti peristiwa AWS KMS atau peristiwa API Data Amazon RDS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	appsync-logging-enabled	Pastikan bahwa AWS AppSync API telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan, atau 'fieldLogLevel' bukan ERROR atau SEMUA.
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	mq-cloudwatch-audit-logging-diaktifkan	Pastikan pialang Amazon MQ mengaktifkan pencatatan CloudWatch audit Amazon. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	mq-cloudwatch-audit-log-diaktifkan	Pastikan bahwa broker Amazon MQ mengaktif kan pencatatan CloudWatch audit. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	eks-cluster-logging-enabled	Pastikan klaster Amazon Elastic Kubernetes Service (Amazon EKS) dikonfigurasi dengan logging diaktifkan. Aturannya adalah NON_COMPLIANT jika logging untuk klaster Amazon EKS tidak diaktifkan untuk semua jenis log.
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	elastic-beanstalk-logs-to-jam tangan awan	Pastikan lingkungan AWS Elastic Beanstalk dikonfigurasi untuk mengirim log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika nilai `StreamLogs` salah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	step-functions-state-machine-logging-diaktifkan	Pastikan bahwa mesin AWS Step Functions telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika mesin status tidak mengaktifkan logging atau konfigurasi logging tidak pada tingkat minimum yang disediakan.
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	netfw-logging-enabled	Pastikan firewall AWS Network Firewall telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika jenis logging tidak dikonfigurasi. Anda dapat menentukan jenis logging yang Anda ingin aturan untuk memeriksa.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	cw-loggroup-retention-period-periksa	Pastikan periode CloudWatch LogGroup retensi Amazon diatur ke lebih dari 365 hari atau periode retensi tertentu. Aturannya adalah NON_COMPLIANT jika periode retensi kurang dari MinRetentionTime, jika ditentukan, atau 365 hari.
6.3.3	Kerentanan keamanan diidentifikasi dan ditangani. (PCI-DSS-V4.0)	lambda-function-settings-check	Pastikan setelan fungsi AWS Lambda untuk runtime, role, timeout, dan ukuran memori sesuai dengan nilai yang diharapkan. Aturan mengabaikan fungsi dengan tipe paket 'Gambar' dan fungsi dengan runtime disetel ke 'OS-Only Runtime'. Aturannya adalah NON_COMPLIANT jika pengaturan fungsi Lambda tidak cocok dengan nilai yang diharapkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.3.3	Kerentanan keamanan diidentif ikasi dan ditangani. (PCI-DSS-V4.0)	eks-cluster-oldest-supported-versi	Pastikan klaster Amazon Elastic Kubernetes Service (EKS) tidak menjalank an versi tertua yang didukung. Aturannya adalah NON_COMPL IANT jika kluster EKS menjalankan versi tertua yang didukung (sama dengan parameter "oldestVersionSup ported).
6.4.1	Aplikasi web yang menghadap publik dilindungi dari serangan. (PCI-DSS-V4.0)	appsync-associated-with-waf	Pastikan AWS AppSync APIs yang terkait dengan daftar kontrol akses AWS WAFv2 web (ACLs). Aturannya adalah NON_COMPLIANT untuk AWS AppSync API jika tidak terkait dengan ACL web.
6.4.1	Aplikasi web yang menghadap publik dilindungi dari serangan. (PCI-DSS-V4.0)	wafv2- webacl-not-empty	Pastikan bahwa ACL WAFv2 Web berisi aturan WAF atau grup aturan WAF. Aturan ini NON_COMPL IANT jika ACL Web tidak berisi aturan WAF atau grup aturan WAF.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.4.1	Aplikasi web yang menghadap publik dilindungi dari serangan. (PCI-DSS-V4.0)	wafv2- rulegroup-not-empty	Pastikan bahwa Grup WAFv2 Aturan berisi aturan. Aturannya adalah NON_COMPLIANT jika tidak ada aturan dalam Grup Aturan. WAFv2
6.4.2	Aplikasi web yang menghadap publik dilindungi dari serangan. (PCI-DSS-V4.0)	appsync-associated-with-waf	Pastikan AWS AppSync APIs yang terkait dengan daftar kontrol akses AWS WAFv2 web (ACLs). Aturannya adalah NON_COMPLIANT untuk AWS AppSync API jika tidak terkait dengan ACL web.
6.4.2	Aplikasi web yang menghadap publik dilindungi dari serangan. (PCI-DSS-V4.0)	wafv2- webacl-not-empty	Pastikan bahwa ACL WAFv2 Web berisi aturan WAF atau grup aturan WAF. Aturan ini NON_COMPLIANT jika ACL Web tidak berisi aturan WAF atau grup aturan WAF.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.4.2	Aplikasi web yang menghadap publik dilindungi dari serangan. (PCI-DSS-V4.0)	wafv2- rulegroup-not-empty	Pastikan bahwa Grup WAFv2 Aturan berisi aturan. Aturannya adalah NON_COMPLIANT jika tidak ada aturan dalam Grup Aturan. WAFv2
6.5.5	Perubahan pada semua komponen sistem dikelola dengan aman. (PCI-DSS-V4.0)	codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan	Pastikan bahwa grup penyebaran untuk Lambda Compute Platform tidak menggunakan konfigurasi penerapan default. Aturannya adalah NON_COMPLIANT jika grup penerapan menggunakan konfigurasi penerapan '. CodeDeployDefaultLambdaAllAtOnce'.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.5.6	Perubahan pada semua komponen sistem dikelola dengan aman. (PCI-DSS-V4.0)	codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan	Pastikan bahwa grup penyebaran untuk Lambda Compute Platform tidak menggunakan konfigurasi penerapan default. Aturannya adalah NON_COMPLIANT jika grup penerapan menggunakan konfigurasi penerapan '. CodeDeployDefaultLambdaAllAtOnce'.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.1	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	s3- bucket-blacklisted-actions-prohibited	Pastikan kebijakan bucket Amazon Simple Storage Service (Amazon S3) tidak mengizinkan tindakan tingkat ember dan tingkat objek yang diblokir pada sumber daya dalam bucket untuk prinsipal dari akun lain. AWS Misalnya, aturan memeriksa bahwa kebijakan bucket Amazon S3 tidak mengizinkan AWS akun lain untuk melakukan tindakan s3: GetBucket * dan s3: DeleteObject pada objek apa pun di bucket. Aturannya adalah NON_COMPLIANT jika ada tindakan yang diblokir yang diizinkan oleh kebijakan bucket Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.1	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	s3- bucket-policy-not-more -permisif	Pastikan kebijakan bucket Amazon Simple Storage Service (S3) Anda tidak mengizinkan izin antar akun selain kebijakan bucket Amazon S3 kontrol yang Anda berikan.
7.2.1	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	iam-policy-in-use	Pastikan bahwa ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.1	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	neptune-cluster-iam-database-otentikasi	Pastikan klaster AWS Amazon Neptune mengaktif kan otentikasi database Identity and Access Managemen t (IAM) and Access Management (IAM). Aturannya adalah NON_COMPL IANT jika klaster Amazon Neptunus tidak mengaktifkan autentikasi database IAM.
7.2.1	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	ec2- instance-profile-a ttached	Pastikan bahwa sebuah EC2 instans memiliki profil AWS Identity and Access Managemen t (IAM) yang melekat padanya. Aturannya adalah NON_COMPL IANT jika tidak ada profil IAM yang dilampirkan ke instance. EC2

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.1	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan brankas cadangan memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Aturannya adalah NON_COMPLIANT jika Brankas Cadangan tidak memiliki kebijakan berbasis sumber daya atau memiliki kebijakan tanpa pernyataan 'Deny' yang sesuai (pernyataan dengan cadangan: DeleteRecoveryPoint, cadangan:, dan cadangan: izin). UpdateRecoveryPointLifecycle PutBackupVaultAccessPolicy

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.2	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	s3- bucket-blacklisted-actions-prohibited	Pastikan kebijakan bucket Amazon Simple Storage Service (Amazon S3) tidak mengizinkan tindakan tingkat ember dan tingkat objek yang diblokir pada sumber daya dalam bucket untuk prinsipal dari akun lain. AWS Misalnya, aturan memeriksa bahwa kebijakan bucket Amazon S3 tidak mengizinkan AWS akun lain untuk melakukan tindakan s3: GetBucket * dan s3: DeleteObject pada objek apa pun di bucket. Aturannya adalah NON_COMPLIANT jika ada tindakan yang diblokir yang diizinkan oleh kebijakan bucket Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.2	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	s3- bucket-policy-not-more -permisif	Pastikan kebijakan bucket Amazon Simple Storage Service (S3) Anda tidak mengizinkan izin antar akun selain kebijakan bucket Amazon S3 kontrol yang Anda berikan.
7.2.2	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	iam-policy-in-use	Pastikan bahwa ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.2	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	neptune-cluster-iam-database-otentikasi	Pastikan klaster AWS Amazon Neptune mengaktif kan otentikasi database Identity and Access Managemen t (IAM) and Access Management (IAM). Aturannya adalah NON_COMPL IANT jika klaster Amazon Neptunus tidak mengaktifkan autentikasi database IAM.
7.2.2	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	ec2- instance-profile-a ttached	Pastikan bahwa sebuah EC2 instans memiliki profil AWS Identity and Access Managemen t (IAM) yang melekat padanya. Aturannya adalah NON_COMPL IANT jika tidak ada profil IAM yang dilampirkan ke instance. EC2

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.2	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan brankas cadangan memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Aturannya adalah NON_COMPLIANT jika Brankas Cadangan tidak memiliki kebijakan berbasis sumber daya atau memiliki kebijakan tanpa pernyataan 'Deny' yang sesuai (pernyataan dengan cadangan: DeleteRecoveryPoint, cadangan:, dan cadangan: izin). UpdateRecoveryPointLifecycle PutBackupVaultAccessPolicy

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.4	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	secretsmanager-secret-unused	Pastikan AWS rahasia Secrets Manager telah diakses dalam beberapa hari tertentu. Aturannya adalah NON_COMPLIANT jika rahasia belum diakses dalam jumlah hari unusedForDays ". Nilai defaultnya adalah 90 hari.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.5	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	s3- bucket-blacklisted-actions-prohibited	Pastikan kebijakan bucket Amazon Simple Storage Service (Amazon S3) tidak mengizinkan tindakan tingkat ember dan tingkat objek yang diblokir pada sumber daya dalam bucket untuk prinsipal dari akun lain. AWS Misalnya, aturan memeriksa bahwa kebijakan bucket Amazon S3 tidak mengizinkan AWS akun lain untuk melakukan tindakan s3: GetBucket * dan s3: DeleteObject pada objek apa pun di bucket. Aturannya adalah NON_COMPLIANT jika ada tindakan yang diblokir yang diizinkan oleh kebijakan bucket Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.5	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	s3- bucket-policy-not-more -permisif	Pastikan kebijakan bucket Amazon Simple Storage Service (S3) Anda tidak mengizinkan izin antar akun selain kebijakan bucket Amazon S3 kontrol yang Anda berikan.
7.2.5	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	iam-policy-in-use	Pastikan bahwa ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.5	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	neptune-cluster-iam-database-otentikasi	Pastikan klaster AWS Amazon Neptune mengaktif kan otentikasi database Identity and Access Managemen t (IAM) and Access Management (IAM). Aturannya adalah NON_COMPL IANT jika klaster Amazon Neptunus tidak mengaktifkan autentikasi database IAM.
7.2.5	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	ec2- instance-profile-a ttached	Pastikan bahwa sebuah EC2 instans memiliki profil AWS Identity and Access Managemen t (IAM) yang melekat padanya. Aturannya adalah NON_COMPL IANT jika tidak ada profil IAM yang dilampirkan ke instance. EC2

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.5	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan brankas cadangan memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Aturannya adalah NON_COMPLIANT jika Brankas Cadangan tidak memiliki kebijakan berbasis sumber daya atau memiliki kebijakan tanpa pernyataan 'Deny' yang sesuai (pernyataan dengan cadangan: DeleteRecoveryPoint, cadangan:, dan cadangan: izin). UpdateRecoveryPointLifecycle PutBackupVaultAccessPolicy

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.5.1	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	secretsmanager-secret-unused	Pastikan AWS rahasia Secrets Manager telah diakses dalam beberapa hari tertentu. Aturannya adalah NON_COMPLIANT jika rahasia belum diakses dalam jumlah hari unusedForDays ". Nilai defaultnya adalah 90 hari.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.6	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	s3- bucket-blacklisted-actions-prohibited	Pastikan kebijakan bucket Amazon Simple Storage Service (Amazon S3) tidak mengizinkan tindakan tingkat ember dan tingkat objek yang diblokir pada sumber daya dalam bucket untuk prinsipal dari akun lain. AWS Misalnya, aturan memeriksa bahwa kebijakan bucket Amazon S3 tidak mengizinkan AWS akun lain untuk melakukan tindakan s3: GetBucket * dan s3: DeleteObject pada objek apa pun di bucket. Aturannya adalah NON_COMPLIANT jika ada tindakan yang diblokir yang diizinkan oleh kebijakan bucket Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.6	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	s3- bucket-policy-not-more -permisif	Pastikan kebijakan bucket Amazon Simple Storage Service (S3) Anda tidak mengizinkan izin antar akun selain kebijakan bucket Amazon S3 kontrol yang Anda berikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.1	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	s3- bucket-blacklisted-actions-prohibited	Pastikan kebijakan bucket Amazon Simple Storage Service (Amazon S3) tidak mengizinkan tindakan tingkat ember dan tingkat objek yang diblokir pada sumber daya dalam bucket untuk prinsipal dari akun lain. AWS Misalnya, aturan memeriksa bahwa kebijakan bucket Amazon S3 tidak mengizinkan AWS akun lain untuk melakukan tindakan s3: GetBucket * dan s3: DeleteObject pada objek apa pun di bucket. Aturannya adalah NON_COMPLIANT jika ada tindakan yang diblokir yang diizinkan oleh kebijakan bucket Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.1	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	s3- bucket-policy-not-more -permisif	Pastikan kebijakan bucket Amazon Simple Storage Service (S3) Anda tidak mengizinkan izin antar akun selain kebijakan bucket Amazon S3 kontrol yang Anda berikan.
7.3.1	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	iam-policy-in-use	Pastikan bahwa ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.1	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	neptune-cluster-iam-database-otentikasi	Pastikan klaster AWS Amazon Neptune mengaktif kan otentikasi database Identity and Access Managemen t (IAM) and Access Management (IAM). Aturannya adalah NON_COMPL IANT jika klaster Amazon Neptunus tidak mengaktifkan autentikasi database IAM.
7.3.1	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	ec2- instance-profile-a ttached	Pastikan bahwa sebuah EC2 instans memiliki profil AWS Identity and Access Managemen t (IAM) yang melekat padanya. Aturannya adalah NON_COMPL IANT jika tidak ada profil IAM yang dilampirkan ke instance. EC2

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.1	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan brankas cadangan memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Aturannya adalah NON_COMPLIANT jika Brankas Cadangan tidak memiliki kebijakan berbasis sumber daya atau memiliki kebijakan tanpa pernyataan 'Deny' yang sesuai (pernyataan dengan cadangan: DeleteRecoveryPoint, cadangan:, dan cadangan: izin). UpdateRecoveryPointLifecycle PutBackupVaultAccessPolicy

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.2	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	s3- bucket-blacklisted-actions-prohibited	Pastikan kebijakan bucket Amazon Simple Storage Service (Amazon S3) tidak mengizinkan tindakan tingkat ember dan tingkat objek yang diblokir pada sumber daya dalam bucket untuk prinsipal dari akun lain. AWS Misalnya, aturan memeriksa bahwa kebijakan bucket Amazon S3 tidak mengizinkan AWS akun lain untuk melakukan tindakan s3: GetBucket * dan s3: DeleteObject pada objek apa pun di bucket. Aturannya adalah NON_COMPLIANT jika ada tindakan yang diblokir yang diizinkan oleh kebijakan bucket Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.2	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	s3- bucket-policy-not-more -permisif	Pastikan kebijakan bucket Amazon Simple Storage Service (S3) Anda tidak mengizinkan izin antar akun selain kebijakan bucket Amazon S3 kontrol yang Anda berikan.
7.3.2	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	iam-policy-in-use	Pastikan bahwa ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.2	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	neptune-cluster-iam-database-otentikasi	Pastikan klaster AWS Amazon Neptune mengaktif kan otentikasi database Identity and Access Managemen t (IAM) and Access Management (IAM). Aturannya adalah NON_COMPL IANT jika klaster Amazon Neptunus tidak mengaktifkan autentikasi database IAM.
7.3.2	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	ec2- instance-profile-a ttached	Pastikan bahwa sebuah EC2 instans memiliki profil AWS Identity and Access Management (IAM) yang dilampirkan padanya. Aturannya adalah NON_COMPL IANT jika tidak ada profil IAM yang dilampirkan ke instance. EC2

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.2	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan brankas cadangan memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Aturannya adalah NON_COMPLIANT jika Brankas Cadangan tidak memiliki kebijakan berbasis sumber daya atau memiliki kebijakan tanpa pernyataan 'Deny' yang sesuai (pernyataan dengan cadangan: DeleteRecoveryPoint, cadangan:, dan cadangan: izin). UpdateRecoveryPointLifecycle PutBackupVaultAccessPolicy

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.3	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	s3- bucket-blacklisted-actions-prohibited	Pastikan kebijakan bucket Amazon Simple Storage Service (Amazon S3) tidak mengizinkan tindakan tingkat ember dan tingkat objek yang diblokir pada sumber daya dalam bucket untuk prinsipal dari akun lain. AWS Misalnya, aturan memeriksa bahwa kebijakan bucket Amazon S3 tidak mengizinkan AWS akun lain untuk melakukan tindakan s3: GetBucket * dan s3: DeleteObject pada objek apa pun di bucket. Aturannya adalah NON_COMPLIANT jika ada tindakan yang diblokir yang diizinkan oleh kebijakan bucket Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.3	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	s3- bucket-policy-not-more -permisif	Pastikan kebijakan bucket Amazon Simple Storage Service (S3) Anda tidak mengizinkan izin antar akun selain kebijakan bucket Amazon S3 kontrol yang Anda berikan.
7.3.3	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	iam-policy-in-use	Pastikan bahwa ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.3	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	neptune-cluster-iam-database-otentikasi	Pastikan klaster AWS Amazon Neptune mengaktif kan otentikasi database Identity and Access Managemen t (IAM) and Access Management (IAM). Aturannya adalah NON_COMPL IANT jika klaster Amazon Neptunus tidak mengaktifkan autentikasi database IAM.
7.3.3	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	ec2- instance-profile-a ttached	Pastikan bahwa sebuah EC2 instans memiliki profil AWS Identity and Access Management (IAM) yang dilampirkan padanya. Aturannya adalah NON_COMPL IANT jika tidak ada profil IAM yang dilampirkan ke instance. EC2

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.3	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan brankas cadangan memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Aturannya adalah NON_COMPLIANT jika Brankas Cadangan tidak memiliki kebijakan berbasis sumber daya atau memiliki kebijakan tanpa pernyataan 'Deny' yang sesuai (pernyataan dengan cadangan: DeleteRecoveryPoint, cadangan:, dan cadangan: izin). UpdateRecoveryPointLifecycle PutBackupVaultAccessPolicy
8.2.1	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	iam-policy-in-use	Pastikan bahwa ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.1	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	ec2- no-amazon-key-pair	Pastikan instans Amazon Elastic Compute Cloud (EC2) yang menjalank an tidak diluncurk an menggunakan pasangan kunci amazon. Aturannya adalah NON_COMPL IANT jika EC2 instance yang sedang berjalan diluncurkan dengan key pair.
8.2.2	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	iam-policy-in-use	Pastikan bahwa ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.2	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	ec2- no-amazon-key-pair	Pastikan instans Amazon Elastic Compute Cloud (EC2) yang menjalank an tidak diluncurk an menggunakan pasangan kunci amazon. Aturannya adalah NON_COMPL IANT jika EC2 instance yang sedang berjalan diluncurkan dengan key pair.
8.2.2	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	codebuild-project-envvar-awscred-per iksa	Pastikan bahwa proyek TIDAK berisi variabel lingkunga n AWS_ACCES S_KEY_ID dan AWS_SECRET _ACCESS_KEY. Aturannya adalah NON_COMPLIANT ketika variabel lingkungan proyek berisi kredensyal teks biasa.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.2	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	secretsmanager-scheduled-rotation-success-periksa	Pastikan AWS rahasia Secrets Manager diputar dengan sukses sesuai dengan jadwal rotasi. Secrets Manager menghitung tanggal rotasi harus terjadi. Aturannya adalah NON_COMPLIANT jika tanggal berlalu dan rahasianya tidak diputar.
8.2.2	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	secretsmanager-secret-periodic-rotation	Pastikan AWS rahasia Secrets Manager telah dirotasi dalam jumlah hari yang ditentukan sebelumnya. Aturannya adalah NON_COMPLIANT jika rahasia belum diputar selama lebih dari jumlah hari maxDaysSinceRotasi. Nilai defaultnya adalah 90 hari.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.2	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	secretsmanager-secret-unused	Pastikan AWS rahasia Secrets Manager telah diakses dalam beberapa hari tertentu. Aturannya adalah NON_COMPLIANT jika rahasia belum diakses dalam jumlah hari unusedForDays ". Nilai defaultnya adalah 90 hari.
8.2.4	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	iam-policy-in-use	Pastikan bahwa ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.4	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	ec2- no-amazon-key-pair	Pastikan instans Amazon Elastic Compute Cloud (EC2) yang menjalank an tidak diluncurk an menggunakan pasangan kunci amazon. Aturannya adalah NON_COMPL IANT jika EC2 instance yang sedang berjalan diluncurkan dengan key pair.
8.2.5	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	iam-policy-in-use	Pastikan bahwa ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.5	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	ec2- no-amazon-key-pair	Pastikan instans Amazon Elastic Compute Cloud (EC2) yang menjalank an tidak diluncurk an menggunakan pasangan kunci amazon. Aturannya adalah NON_COMPL IANT jika EC2 instance yang sedang berjalan diluncurkan dengan key pair.
8.2.6	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	secretsmanager-sec ret-unused	Pastikan AWS rahasia Secrets Manager telah diakses dalam beberapa hari tertentu. Aturannya adalah NON_COMPL IANT jika rahasia belum diakses dalam jumlah hari unusedFor Days ". Nilai defaultny a adalah 90 hari.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.7	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	s3- bucket-blacklisted-actions-prohibited	Pastikan kebijakan bucket Amazon Simple Storage Service (Amazon S3) tidak mengizinkan tindakan tingkat ember dan tingkat objek yang diblokir pada sumber daya dalam bucket untuk prinsipal dari akun lain. AWS Misalnya, aturan memeriksa bahwa kebijakan bucket Amazon S3 tidak mengizinkan AWS akun lain untuk melakukan tindakan s3: GetBucket * dan s3: DeleteObject pada objek apa pun di bucket. Aturannya adalah NON_COMPLIANT jika ada tindakan yang diblokir yang diizinkan oleh kebijakan bucket Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.7	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	s3- bucket-policy-not-more -permisif	Pastikan kebijakan bucket Amazon Simple Storage Service (S3) Anda tidak mengizinkan izin antar akun selain kebijakan bucket Amazon S3 kontrol yang Anda berikan.
8.2.7	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	iam-policy-in-use	Pastikan bahwa ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.7	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	neptune-cluster-iam-database-otentikasi	Pastikan klaster AWS Amazon Neptune mengaktif kan otentikasi database Identity and Access Managemen t (IAM) and Access Management (IAM). Aturannya adalah NON_COMPL IANT jika klaster Amazon Neptunus tidak mengaktifkan autentikasi database IAM.
8.2.7	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	ec2- instance-profile-attached	Pastikan bahwa sebuah EC2 instans memiliki profil AWS Identity and Access Management (IAM) yang dilampirkan padanya. Aturannya adalah NON_COMPL IANT jika tidak ada profil IAM yang dilampirkan ke instance. EC2

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.7	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan brankas cadangan memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Aturannya adalah NON_COMPLIANT jika Brankas Cadangan tidak memiliki kebijakan berbasis sumber daya atau memiliki kebijakan tanpa pernyataan 'Deny' yang sesuai (pernyataan dengan cadangan: DeleteRecoveryPoint, cadangan:, dan cadangan: izin). UpdateRecoveryPointLifecycle PutBackupVaultAccessPolicy

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.8	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	s3- bucket-blacklisted-actions-prohibited	Pastikan kebijakan bucket Amazon Simple Storage Service (Amazon S3) tidak mengizinkan tindakan tingkat ember dan tingkat objek yang diblokir pada sumber daya dalam bucket untuk prinsipal dari akun lain. AWS Misalnya, aturan memeriksa bahwa kebijakan bucket Amazon S3 tidak mengizinkan AWS akun lain untuk melakukan tindakan s3: GetBucket * dan s3: DeleteObject pada objek apa pun di bucket. Aturannya adalah NON_COMPLIANT jika ada tindakan yang diblokir yang diizinkan oleh kebijakan bucket Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.8	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	s3- bucket-policy-not-more -permisif	Pastikan kebijakan bucket Amazon Simple Storage Service (S3) Anda tidak mengizinkan izin antar akun selain kebijakan bucket Amazon S3 kontrol yang Anda berikan.
8.2.8	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	iam-policy-in-use	Pastikan bahwa ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.8	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	neptune-cluster-iam-database-otentikasi	Pastikan klaster AWS Amazon Neptune mengaktif kan otentikasi database Identity and Access Managemen t (IAM) and Access Management (IAM). Aturannya adalah NON_COMPL IANT jika klaster Amazon Neptunus tidak mengaktifkan autentikasi database IAM.
8.2.8	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	ec2-imdsv2-periksa	Pastikan versi metadata instans Amazon Elastic Compute Cloud (Amazon EC2) Anda dikonfigurasi dengan Instance Metadata Service Version 2 (). IMDSv2 Aturannya adalah NON_COMPL IANT jika HttpTokens disetel ke opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.8	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	ec2- instance-profile-attached	Pastikan bahwa sebuah EC2 instans memiliki profil AWS Identity and Access Management (IAM) yang dilampirkan padanya. Aturannya adalah NON_COMPLIANT jika tidak ada profil IAM yang dilampirkan ke instance. EC2
8.2.8	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	autoscaling-launchconfig-requires-imdsv2	Pastikan bahwa hanya IMDSv2 diaktifkan. Aturan ini NON_COMPLIANT jika versi Metadata tidak disertakan dalam konfigurasi peluncuran atau jika kedua Metadata V1 dan V2 diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.8	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan brankas cadangan memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Aturannya adalah NON_COMPLIANT jika Brankas Cadangan tidak memiliki kebijakan berbasis sumber daya atau memiliki kebijakan tanpa pernyataan 'Deny' yang sesuai (pernyataan dengan cadangan: DeleteRecoveryPoint, cadangan:, dan cadangan: izin). UpdateRecoveryPointLifecycle PutBackupVaultAccessPolicy

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.10.1	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	access-keys-rotated	Pastikan kunci akses IAM aktif diputar (diubah) dalam jumlah hari yang ditentuka n dalam maxAccess Key Usia. Aturannya adalah NON_COMPL IANT jika kunci akses tidak diputar dalam jangka waktu yang ditentukan. Nilai defaultnya adalah 90 hari.
8.3.10.1	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	secretsmanager-sch eduled-rotation-su ccess-periksa	Pastikan AWS rahasia Secrets Manager diputar dengan sukses sesuai dengan jadwal rotasi. Secrets Manager menghitun g tanggal rotasi harus terjadi. Aturannya adalah NON_COMPL IANT jika tanggal berlalu dan rahasiany a tidak diputar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.10.1	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	secretsmanager-secret-periodic-rotation	Pastikan AWS rahasia Secrets Manager telah dirotasi dalam jumlah hari yang ditentukan sebelumnya. Aturannya adalah NON_COMPLIANT jika rahasia belum diputar selama lebih dari jumlah hari maxDaysSinceRotasi. Nilai defaultnya adalah 90 hari.
8.3.11	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	iam-policy-in-use	Pastikan bahwa ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.11	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	ec2- no-amazon-key-pair	Pastikan instans Amazon Elastic Compute Cloud (EC2) yang menjalank an tidak diluncurk an menggunakan pasangan kunci amazon. Aturannya adalah NON_COMPL IANT jika EC2 instance yang sedang berjalan diluncurkan dengan key pair.
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	athena-workgroup-e ncrypted-at-istirahat	Pastikan bahwa workgroup Amazon Athena dienkripsi saat istirahat. Aturannya adalah NON_COMPL IANT jika enkripsi data saat istirahat tidak diaktifkan untuk workgroup Athena.
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	neptune-cluster-sn apshot-encrypted	Pastikan bahwa kluster Amazon Neptunus DB memiliki snapshot yang dienkripsi. Aturannya adalah NON_COMPL IANT jika cluster Neptunus tidak memiliki snapshot yang dienkripsi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	redshift-cluster-kms-enabled	Pastikan bahwa klaster Amazon Redshift menggunakan AWS kunci Key Management Service (AWS KMS) yang ditentukan untuk enkripsi. Aturannya adalah COMPLIANT jika enkripsi diaktifkan dan cluster dienkripsi dengan kunci yang disediakan dalam parameter. kmsKeyArn Aturannya adalah NON_COMPLIANT jika cluster tidak dienkripsi atau dienkripsi dengan kunci lain.
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	codebuild-project-s3-log-terenkripsi	Pastikan AWS CodeBuild proyek yang dikonfigurasi dengan Amazon S3 Logs mengaktifkan enkripsi untuk lognya. Aturannya adalah NON_COMPLIANT jika 'EncryptionDisabled' disetel ke 'true' dalam S3 proyek. LogsConfig CodeBuild

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	dms-redis-tls-enabled	Pastikan titik akhir AWS Database Migration Service (AWS DMS) untuk penyimpanan data Redis diaktifkan untuk TLS/SSL encryption of data communicated with other endpoints. The rule is NON_COMPLIANT if TLS/SSL enkripsi tidak diaktifkan.
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	eks-secrets-encrypted	Pastikan bahwa klaster Amazon Elastic Kubernetes Service dikonfigurasi agar rahasia Kubernetes dienkripsi menggunakan kunci Key Management Service (KMS). AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	api-gw-cache-enabled-dan-dienkripsi	Pastikan bahwa semua metode dalam tahapan Amazon API Gateway telah mengaktifkan cache dan cache dienkrips i. Aturannya adalah NON_COMPLIANT jika metode apa pun dalam tahap Amazon API Gateway tidak dikonfigurasi ke cache atau cache tidak dienkripsi.
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	dynamodb-table-encrypted-kms	Pastikan tabel Amazon DynamoDB dienkripsi AWS dengan Key Management Service (KMS). Aturannya adalah NON_COMPLIANT jika tabel Amazon DynamoDB tidak dienkripsi dengan KMS. AWS Aturannya juga NON_COMPLIANT jika kunci AWS KMS terenkripsi tidak ada dalam parameter input. kmsKeyArns

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	codebuild-project-envvar-awscred-periksa	Pastikan bahwa proyek TIDAK berisi variabel lingkungan AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY. Aturannya adalah NON_COMPLIANT ketika variabel lingkungan proyek berisi kredensyal teks biasa.
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancers . Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	eks-cluster-secrets-encrypted	Pastikan bahwa klaster Amazon EKS tidak dikonfigurasi agar rahasia Kubernetes dienkripsi menggunakan KMS. AWS Aturannya adalah NON_COMPLIANT jika kluster EKS tidak memiliki sumber daya EncryptionConfig atau jika EncryptionConfig tidak menyebutkan rahasia sebagai sumber daya.
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	kinesis-stream-encrypted	Pastikan aliran Amazon Kinesis dienkripsi saat istirahat dengan enkripsi sisi server. Aturannya adalah NON_COMPLIANT untuk aliran Kinesis jika " StreamEncryption tidak ada.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	msk-in-cluster-node-membutuhkan-tls	Pastikan bahwa klaster MSK Amazon memberlakukan enkripsi dalam perjalanan menggunakan HTTPS (TLS) dengan node broker klaster. Aturannya adalah NON_COMPLIANT jika komunikasi teks biasa diaktifkan untuk koneksi node broker in-cluster.
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	neptune-cluster-encrypted	Pastikan enkripsi penyimpanan diaktifkan untuk kluster Amazon Neptunus DB Anda. Aturannya adalah NON_COMPLIANT jika enkripsi penyimpanan tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	dms-endpoint-ssl-configured	Pastikan titik akhir AWS Database Migration Service (AWS DMS) dikonfigurasi dengan koneksi SSL. Aturannya adalah NON_COMPLIANT jika AWS DMS tidak memiliki koneksi SSL yang dikonfigurasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.4	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	s3- bucket-blacklisted-actions-prohibited	Pastikan kebijakan bucket Amazon Simple Storage Service (Amazon S3) tidak mengizinkan tindakan tingkat ember dan tingkat objek yang diblokir pada sumber daya dalam bucket untuk prinsipal dari akun lain. AWS Misalnya, aturan memeriksa bahwa kebijakan bucket Amazon S3 tidak mengizinkan AWS akun lain untuk melakukan tindakan s3: GetBucket * dan s3: DeleteObject pada objek apa pun di bucket. Aturannya adalah NON_COMPLIANT jika ada tindakan yang diblokir yang diizinkan oleh kebijakan bucket Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.4	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	s3- bucket-policy-not-more -permisif	Pastikan kebijakan bucket Amazon Simple Storage Service (S3) Anda tidak mengizinkan izin antar akun selain kebijakan bucket Amazon S3 kontrol yang Anda berikan.
8.3.4	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	iam-policy-in-use	Pastikan bahwa ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.4	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	neptune-cluster-iam-database-otentikasi	Pastikan klaster AWS Amazon Neptune mengaktif kan otentikasi database Identity and Access Managemen t (IAM) and Access Management (IAM). Aturannya adalah NON_COMPL IANT jika klaster Amazon Neptunus tidak mengaktifkan autentikasi database IAM.
8.3.4	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	ec2- instance-profile-a ttached	Pastikan bahwa sebuah EC2 instans memiliki profil AWS Identity and Access Management (IAM) yang dilampirkan padanya. Aturannya adalah NON_COMPL IANT jika tidak ada profil IAM yang dilampirkan ke instance. EC2

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.4	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan brankas cadangan memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Aturannya adalah NON_COMPLIANT jika Brankas Cadangan tidak memiliki kebijakan berbasis sumber daya atau memiliki kebijakan tanpa pernyataan 'Deny' yang sesuai (pernyataan dengan cadangan: DeleteRecoveryPoint, cadangan:, dan cadangan: izin). UpdateRecoveryPointLifecycle PutBackupVaultAccessPolicy

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.5	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	access-keys-rotated	Pastikan kunci akses IAM aktif diputar (diubah) dalam jumlah hari yang ditentuka n dalam maxAccess Key Usia. Aturannya adalah NON_COMPL IANT jika kunci akses tidak diputar dalam jangka waktu yang ditentukan. Nilai defaultnya adalah 90 hari.
8.3.5	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	secretsmanager-sch eduled-rotation-su ccess-periksa	Pastikan AWS rahasia Secrets Manager diputar dengan sukses sesuai dengan jadwal rotasi. Secrets Manager menghitun g tanggal rotasi harus terjadi. Aturannya adalah NON_COMPL IANT jika tanggal berlalu dan rahasiany a tidak diputar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.5	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	secretsmanager-secret-periodic-rotation	Pastikan AWS rahasia Secrets Manager telah dirotasi dalam jumlah hari yang ditentukan sebelumnya. Aturannya adalah NON_COMPLIANT jika rahasia belum diputar selama lebih dari jumlah hari maxDaysSince Rotasi. Nilai defaultnya adalah 90 hari.
8.3.7	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	access-keys-rotated	Pastikan kunci akses IAM aktif diputar (diubah) dalam jumlah hari yang ditentukan dalam maxAccess Key Usia. Aturannya adalah NON_COMPLIANT jika kunci akses tidak diputar dalam jangka waktu yang ditentukan. Nilai defaultnya adalah 90 hari.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.7	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	secretsmanager-scheduled-rotation-success-periksa	Pastikan AWS rahasia Secrets Manager diputar dengan sukses sesuai dengan jadwal rotasi. Secrets Manager menghitung tanggal rotasi harus terjadi. Aturannya adalah NON_COMPLIANT jika tanggal berlalu dan rahasianya tidak diputar.
8.3.7	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	secretsmanager-secret-periodic-rotation	Pastikan AWS rahasia Secrets Manager telah dirotasi dalam jumlah hari yang ditentukan sebelumnya. Aturannya adalah NON_COMPLIANT jika rahasia belum diputar selama lebih dari jumlah hari maxDaysSinceRotasi. Nilai defaultnya adalah 90 hari.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.9	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	access-keys-rotated	Pastikan kunci akses IAM aktif diputar (diubah) dalam jumlah hari yang ditentuka n dalam maxAccess Key Usia. Aturannya adalah NON_COMPL IANT jika kunci akses tidak diputar dalam jangka waktu yang ditentukan. Nilai defaultnya adalah 90 hari.
8.3.9	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	secretsmanager-sch eduled-rotation-su ccess-periksa	Pastikan AWS rahasia Secrets Manager diputar dengan sukses sesuai dengan jadwal rotasi. Secrets Manager menghitun g tanggal rotasi harus terjadi. Aturannya adalah NON_COMPL IANT jika tanggal berlalu dan rahasiany a tidak diputar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.9	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	secretsmanager-secret-periodic-rotation	Pastikan AWS rahasia Secrets Manager telah dirotasi dalam jumlah hari yang ditentukan sebelumnya. Aturannya adalah NON_COMPLIANT jika rahasia belum diputar selama lebih dari jumlah hari maxDaysSinceRotasi. Nilai defaultnya adalah 90 hari.
8.4.1	Otentikasi multi-faktor (MFA) diimplementasikan untuk mengamankan akses ke CDE. (PCI-DSS-V4.0)	s3- bucket-mfa-delete-enabled	Pastikan MFA Delete diaktifkan di konfigurasi pembuatan versi bucket Amazon Simple Storage Service (Amazon S3). Aturannya adalah NON_COMPLIANT jika MFA Delete tidak diaktifkan.
8.4.2	Otentikasi multi-faktor (MFA) diimplementasikan untuk mengamankan akses ke CDE. (PCI-DSS-V4.0)	s3- bucket-mfa-delete-enabled	Pastikan MFA Delete diaktifkan di konfigurasi pembuatan versi bucket Amazon Simple Storage Service (Amazon S3). Aturannya adalah NON_COMPLIANT jika MFA Delete tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.4.3	Otentikasi multi-faktor (MFA) diimplementasikan untuk mengamankan akses ke CDE. (PCI-DSS-V4.0)	s3- bucket-mfa-delete-enabled	Pastikan MFA Delete diaktifkan di konfigurasi pembuatan versi bucket Amazon Simple Storage Service (Amazon S3). Aturannya adalah NON_COMPLIANT jika MFA Delete tidak diaktifkan.
8.6.3	Penggunaan akun aplikasi dan sistem serta faktor otentikasi terkait dikelola dengan ketat. (PCI-DSS-V4.0)	access-keys-rotated	Pastikan kunci akses IAM aktif diputar (diubah) dalam jumlah hari yang ditentukan dalam maxAccess Key Usia. Aturannya adalah NON_COMPLIANT jika kunci akses tidak diputar dalam jangka waktu yang ditentukan. Nilai defaultnya adalah 90 hari.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.6.3	Penggunaan akun aplikasi dan sistem serta faktor otentikasi terkait dikelola dengan ketat. (PCI-DSS-V4.0)	secretsmanager-scheduled-rotation-success-periksa	Pastikan AWS rahasia Secrets Manager diputar dengan sukses sesuai dengan jadwal rotasi. Secrets Manager menghitung tanggal rotasi harus terjadi. Aturannya adalah NON_COMPLIANT jika tanggal berlalu dan rahasianya tidak diputar.
8.6.3	Penggunaan akun aplikasi dan sistem serta faktor otentikasi terkait dikelola dengan ketat. (PCI-DSS-V4.0)	secretsmanager-secret-periodic-rotation	Pastikan AWS rahasia Secrets Manager telah dirotasi dalam jumlah hari yang ditentukan sebelumnya. Aturannya adalah NON_COMPLIANT jika rahasia belum diputar selama lebih dari jumlah hari maxDaysSinceRotasi. Nilai defaultnya adalah 90 hari.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.1.2	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	neptune-cluster-snapshot-public-dilarang	Pastikan snapshot cluster DB manual Amazon Neptunus tidak bersifat publik. Aturannya adalah NON_COMPLIANT jika ada snapshot cluster Neptunus yang ada dan yang baru bersifat publik.
A1.1.2	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan brankas cadangan memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Aturannya adalah NON_COMPLIANT jika Brankas Cadangan tidak memiliki kebijakan berbasis sumber daya atau memiliki kebijakan tanpa pernyataan 'Deny' yang sesuai (pernyataan dengan cadangan: DeleteRecoveryPoint, cadangan:, dan cadangan: izin). UpdateRecoveryPointLifecycle PutBackupVaultAccessPolicy

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.1.2	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	emr-block-public-access	Pastikan akun dengan Amazon EMR telah mengaktifkan pengaturan akses publik yang memblokir. Aturannya adalah NON_COMPLIANT jika BlockPublicSecurityGroupRules salah, atau jika benar, port selain Port 22 terdaftar di. PermittedPublicSecurityGroupRuleRanges
A1.1.2	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	s3- -blok access-point-public-access	Pastikan jalur akses Amazon S3 telah mengaktifkan pengaturan akses publik blokir. Aturannya adalah NON_COMPLIANT jika pengaturan akses publik blok tidak diaktifkan untuk titik akses S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.1.2	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	s3- -blok account-level-public-access	Pastikan bahwa pengaturan blok akses publik yang diperlukan dikonfigurasi dari tingkat akun. Aturannya hanya NON_COMPLIANT jika bidang yang ditetapkan di bawah ini tidak cocok dengan bidang yang sesuai di item konfigurasi.
A1.1.2	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	s3- bucket-mfa-delete-enabled	Pastikan MFA Delete diaktifkan di konfigurasi pembuatan versi bucket Amazon Simple Storage Service (Amazon S3). Aturannya adalah NON_COMPLIANT jika MFA Delete tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	api-gw-endpoint-type-periksa	Pastikan Amazon API Gateway APIs adalah tipe yang ditentuka n dalam parameter aturan 'endpoint ConfigurationType'. Aturan mengembal ikan NON_COMPL IANT jika REST API tidak cocok dengan tipe titik akhir yang dikonfigurasi dalam parameter aturan.
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	netfw-policy-default-action-fragmen-paket	Pastikan kebijakan AWS Network Firewall dikonfigurasi dengan tindakan default stateless yang ditentukan pengguna untuk paket terfragme ntasi. Aturannya adalah NON_COMPL IANT jika tindakan default stateless untuk paket terfragmentasi tidak cocok dengan tindakan default yang ditentukan pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	eks-endpoint-no-public-akses	Pastikan titik akhir Amazon Elastic Kubernetes Service (Amazon EKS) tidak dapat diakses publik. Aturannya adalah NON_COMPLIANT jika titik akhir dapat diakses publik.
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	terbatas-ssh	Catatan: Untuk aturan ini, pengidentifikasi aturan (INCOMING_SSH_DISABLED) dan nama aturan (restricted-ssh) berbeda. Pastikan bahwa lalu lintas SSH yang masuk untuk grup keamanan dapat diakses. Aturannya adalah COMPLIANT jika alamat IP dari lalu lintas SSH yang masuk dalam grup keamanan dibatasi (CIDR selain 0.0.0.0/0 atau: :/0). Jika tidak, NON_COMPLIANT.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	appsync-associated-with-waf	Pastikan AWS AppSync APIs yang terkait dengan daftar kontrol akses AWS WAFv2 web (ACLs). Aturannya adalah NON_COMPLIANT untuk AWS AppSync API jika tidak terkait dengan ACL web.
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber Bitbucket TIDAK berisi kredenal masuk atau tidak. Aturannya adalah NON_COMPLIANT jika URL berisi informasi login dan COMPLIANT jika tidak.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancers . Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	emr-block-public-access	Pastikan akun dengan Amazon EMR telah mengaktifkan pengaturan akses publik yang memblokir. Aturannya adalah NON_COMPLIANT jika BlockPublicSecurityGroupRules salah, atau jika benar, port selain Port 22 terdaftar di. PermittedPublicSecurityGroupRuleRanges
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	nacl-no-unrestricted-ssh-rdp	Pastikan port default untuk lalu lintas masuk SSH/RDP untuk daftar kontrol akses jaringan () dibatasi. NACLs Aturannya adalah NON_COMPLIANT jika entri masuk NACL memungkinkan blok sumber TCP atau UDP CIDR untuk port 22 atau 3389.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	ec2- -semua client-vpn-not-authorize	Pastikan bahwa aturan otorisasi AWS Client VPN tidak mengotorisasi akses koneksi untuk semua klien. Aturannya adalah NON_COMPLIANT jika 'AccessAll' hadir dan disetel ke true.
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	internet-gateway-authorized-vpc-hanya	Pastikan gateway internet dilampirkan ke cloud pribadi virtual resmi (Amazon VPC). Aturannya adalah NON_COMPLIANT jika gateway internet dilampirkan ke VPC yang tidak sah.
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	s3- -blok access-point-public-access	Pastikan jalur akses Amazon S3 telah mengaktifkan pengaturan akses publik blokir. Aturannya adalah NON_COMPLIANT jika pengaturan akses publik blok tidak diaktifkan untuk titik akses S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	s3- -blok account-level-public-access	Pastikan bahwa pengaturan blok akses publik yang diperlukan dikonfigurasi dari tingkat akun. Aturannya hanya NON_COMPLIANT jika bidang yang ditetapkan di bawah ini tidak cocok dengan bidang yang sesuai di item konfigurasi.
A1.2.1	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	api-gwv2- access-logs-enabled	Pastikan tahap Amazon API Gateway V2 mengaktifkan pencatatan akses. Aturannya adalah NON_COMPLIANT jika 'accessLogSettings' tidak ada dalam konfigurasi Stage.
A1.2.1	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.2.1	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	cloudtrail-security-trail-enabled	Pastikan bahwa setidaknya ada satu AWS CloudTrail jejak yang ditentukan dengan praktik terbaik keamanan. Aturan ini SESUAI jika setidaknya ada satu jejak yang memenuhi semua hal berikut:
A1.2.1	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	neptune-cluster-cloudwatch-log-ekspor diaktifkan	Pastikan klaster CloudWatch Amazon Neptunus mengaktifkan ekspor log untuk log audit. Aturannya adalah NON_COMPLIANT jika klaster Neptunus tidak mengaktifkan ekspor log untuk log audit. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.2.1	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	ecs-task-definition-log-konfigurasi	Pastikan bahwa LogConfiguration diatur pada Definisi Tugas ECS aktif. Aturan ini NON_COMPLIANT jika ECSTask Definisi aktif tidak memiliki sumber daya LogConfiguration yang ditentukan atau nilai untuk LogConfiguration adalah null dalam setidaknya satu definisi kontainer.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.2.1	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	cloudtrail-diaktifkan	Catatan: Untuk aturan ini, pengidentifikasi aturan (CLOUD_TRAIL_ENABLED) dan nama aturan (cloudtrail-enabled) berbeda. Pastikan AWS CloudTrail jejak diaktifkan di AWS akun Anda. Aturannya adalah NON_COMPLIANT jika jejak tidak diaktifkan. Secara opsional, aturan memeriksa bucket S3 tertentu, topik Amazon Simple Notification Service (Amazon SNS), dan grup log. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.2.1	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	multi-region-cloudtrail-enabled	Catatan: untuk aturan ini, pengidentifikasi aturan (MULTI_REGION_CLOUD_TRAIL_ENABLED) dan nama aturan () berbeda. multi-region-cloudtrail-enabled Pastikan setidaknya ada satu multi-wilayah AWS CloudTrail. Aturannya adalah NON_COMPLIANT jika jejak tidak cocok dengan parameter input. Aturannya adalah NON_COMPLIANT jika ExcludeManagementEventSources bidang tidak kosong atau jika AWS CloudTrail dikonfigurasi untuk mengecualikan peristiwa manajemen seperti peristiwa AWS KMS atau peristiwa API Data Amazon RDS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.2.1	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	appsync-logging-enabled	Pastikan bahwa AWS AppSync API telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan, atau 'fieldLogLevel' bukan ERROR atau SEMUA.
A1.2.1	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	mq-cloudwatch-audit-logging-diaktifkan	Pastikan pialang Amazon MQ mengaktifkan pencatatan CloudWatch audit Amazon. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.
A1.2.1	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	mq-cloudwatch-audit-log-diaktifkan	Pastikan bahwa broker Amazon MQ mengaktifkan pencatatan CloudWatch audit. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.2.1	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	eks-cluster-logging-enabled	Pastikan klaster Amazon Elastic Kubernetes Service (Amazon EKS) dikonfigurasi dengan logging diaktifkan. Aturannya adalah NON_COMPLIANT jika logging untuk klaster Amazon EKS tidak diaktifkan untuk semua jenis log.
A1.2.1	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	elastic-beanstalk-logs-to-jam tangan awan	Pastikan lingkungan AWS Elastic Beanstalk dikonfigurasi untuk mengirim log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika nilai `StreamLogs` salah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.2.1	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	step-functions-state-machine-logging-diaktifkan	Pastikan bahwa mesin AWS Step Functions telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika mesin status tidak mengaktifkan logging atau konfigurasi logging tidak pada tingkat minimum yang disediakan.
A1.2.1	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	netfw-logging-enabled	Pastikan firewall AWS Network Firewall telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika jenis logging tidak dikonfigurasi. Anda dapat menentukan jenis logging yang Anda ingin aturan untuk memeriksa.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.2.3	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	security-account-information-provided	Pastikan bahwa Anda telah memberikan informasi kontak keamanan untuk kontak AWS akun Anda. Aturannya adalah NON_COMPLIANT jika informasi kontak keamanan dalam akun tidak disediakan.
A3.2.5.1	Cakupan PCI DSS didokumentasikan dan divalidasi. (PCI-DSS-V4.0)	macie-auto-sensitive-data-penemuan-cek	Pastikan penemuan data sensitif otomatis diaktifkan untuk Amazon Macie. Aturannya adalah NON_COMPLIANT jika penemuan data sensitif otomatis dinonaktifkan. Aturan ini BERLAKU untuk akun administrator dan NOT_APPLICABLE untuk akun anggota.
A3.2.5.1	Cakupan PCI DSS didokumentasikan dan divalidasi. (PCI-DSS-V4.0)	macie-status-check	Pastikan Amazon Macie diaktifkan di akun Anda per wilayah. Aturannya adalah NON_COMPLIANT jika atribut 'status' tidak disetel ke 'ENABLED'.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.2.5.2	Cakupan PCI DSS didokumentasikan dan divalidasi. (PCI-DSS-V4.0)	macie-auto-sensitive-data-penemuan-cek	Pastikan penemuan data sensitif otomatis diaktifkan untuk Amazon Macie. Aturannya adalah NON_COMPLIANT jika penemuan data sensitif otomatis dinonaktifkan. Aturan ini BERLAKU untuk akun administrator dan NOT_APPLI CABLE untuk akun anggota.
A3.2.5.2	Cakupan PCI DSS didokumentasikan dan divalidasi. (PCI-DSS-V4.0)	macie-status-check	Pastikan Amazon Macie diaktifkan di akun Anda per wilayah. Aturannya adalah NON_COMPL IANT jika atribut 'status' tidak disetel ke 'ENABLED'.
A3.3.1	PCI DSS dimasukka n ke dalam kegiatan business-as-usual (BAU). (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifka n di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.3.1	PCI DSS dimasukkan ke dalam kegiatan business-as-usual (BAU). (PCI-DSS-V4.0)	ec2- instance-detailed-monitoring-enabled	Pastikan pemantauan terperinci diaktifkan untuk EC2 instans. Aturannya adalah NON_COMPLIANT jika pemantauan terperinci tidak diaktifkan.
A3.3.1	PCI DSS dimasukkan ke dalam kegiatan business-as-usual (BAU). (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.3.1	PCI DSS dimasukkan ke dalam kegiatan business-as-usual (BAU). (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.3.1	PCI DSS dimasukkan ke dalam kegiatan business-as-usual (BAU). (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.3.1	PCI DSS dimasukkan ke dalam kegiatan business-as-usual (BAU). (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.
A3.3.1	PCI DSS dimasukkan ke dalam kegiatan business-as-usual (BAU). (PCI-DSS-V4.0)	cloudwatch-alarm-resource-check	Pastikan bahwa jenis sumber daya memiliki CloudWatch alarm untuk metrik bernama. Untuk jenis sumber daya, Anda dapat menentukan volume EBS, EC2 instans, kluster Amazon RDS, atau bucket S3. Aturannya SESUAI jika metrik bernama memiliki ID sumber daya dan CloudWatch alarm.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.3.1	PCI DSS dimasukkan ke dalam kegiatan business-as-usual (BAU). (PCI-DSS-V4.0)	cloudwatch-alarm-settings-check	Pastikan CloudWatch alarm dengan nama metrik yang diberikan memiliki pengaturan yang ditentukan.
A3.3.1	PCI DSS dimasukkan ke dalam kegiatan business-as-usual (BAU). (PCI-DSS-V4.0)	wafv2- rulegroup-logging-enabled	Pastikan pengumpulan metrik CloudWatch keamanan Amazon pada grup AWS WAFv2 aturan diaktifkan. Aturannya adalah NON_COMPLIANT jika '. VisibilityConfig CloudWatchMetricsEnabled'bidang disetel ke false.
A3.3.1	PCI DSS dimasukkan ke dalam kegiatan business-as-usual (BAU). (PCI-DSS-V4.0)	sns-topic-message-delivery-notifikasi-diaktifkan	Pastikan pencatatan Amazon Simple Notification Service (SNS) diaktifkan untuk status pengiriman pesan notifikasi yang dikirim ke topik untuk titik akhir. Aturannya adalah NON_COMPLIANT jika pemberitahuan status pengiriman untuk pesan tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.4.1	Akses logis ke lingkungan data pemegang kartu dikendalikan dan dikelola. (PCI-DSS-V4.0)	neptune-cluster-snapshot-public-dilarang	Pastikan snapshot cluster DB manual Amazon Neptunus tidak bersifat publik. Aturannya adalah NON_COMPLIANT jika ada snapshot cluster Neptunus yang ada dan yang baru bersifat publik.
A3.4.1	Akses logis ke lingkungan data pemegang kartu dikendalikan dan dikelola. (PCI-DSS-V4.0)	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan brankas cadangan memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Aturannya adalah NON_COMPLIANT jika Brankas Cadangan tidak memiliki kebijakan berbasis sumber daya atau memiliki kebijakan tanpa pernyataan 'Deny' yang sesuai (pernyataan dengan cadangan: DeleteRecoveryPoint, cadangan:, dan cadangan: izin). UpdateRecoveryPointLifecycle PutBackupVaultAccessPolicy

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.4.1	Akses logis ke lingkungan data pemegang kartu dikendalikan dan dikelola. (PCI-DSS-V4.0)	emr-block-public-access	Pastikan akun dengan Amazon EMR telah mengaktifkan pengaturan akses publik yang memblokir. Aturannya adalah NON_COMPLIANT jika BlockPublicSecurityGroupRules salah, atau jika benar, port selain Port 22 terdaftar di. PermittedPublicSecurityGroupRuleRanges
A3.4.1	Akses logis ke lingkungan data pemegang kartu dikendalikan dan dikelola. (PCI-DSS-V4.0)	secretsmanager-secret-unused	Pastikan AWS rahasia Secrets Manager telah diakses dalam beberapa hari tertentu. Aturannya adalah NON_COMPLIANT jika rahasia belum diakses dalam jumlah hari unusedForDays ". Nilai defaultnya adalah 90 hari.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.4.1	Akses logis ke lingkungan data pemegang kartu dikendalikan dan dikelola. (PCI-DSS-V4.0)	s3- -blok access-point-public-access	Pastikan jalur akses Amazon S3 telah mengaktif kan pengaturan akses publik blokir. Aturannya adalah NON_COMPLIANT jika pengaturan akses publik blok tidak diaktifkan untuk titik akses S3.
A3.4.1	Akses logis ke lingkungan data pemegang kartu dikendalikan dan dikelola. (PCI-DSS-V4.0)	s3- -blok account-level-public-access	Pastikan bahwa pengaturan blok akses publik yang diperlukan dikonfigu rasi dari tingkat akun. Aturannya hanya NON_COMPLIANT jika bidang yang ditetapkan di bawah ini tidak cocok dengan bidang yang sesuai di item konfigurasi.
A3.4.1	Akses logis ke lingkungan data pemegang kartu dikendalikan dan dikelola. (PCI-DSS-V4.0)	s3- bucket-mfa-delete-enabled	Pastikan MFA Delete diaktifkan di konfigura si pembuatan versi bucket Amazon Simple Storage Service (Amazon S3). Aturannya adalah NON_COMPLIANT jika MFA Delete tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.5.1	Peristiwa mencurigakan diidentifikasi dan ditanggapi. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
A3.5.1	Peristiwa mencurigakan diidentifikasi dan ditanggapi. (PCI-DSS-V4.0)	ec2- instance-detailed-monitoring-enabled	Pastikan pemantauan terperinci diaktifkan untuk EC2 instans. Aturannya adalah NON_COMPLIANT jika pemantauan terperinci tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.5.1	Peristiwa mencurigakan diidentifikasi dan ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.5.1	Peristiwa mencurigakan diidentifikasi dan ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.5.1	Peristiwa mencurigakan diidentifikasi dan ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.5.1	Peristiwa mencurigakan diidentifikasi dan ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.
A3.5.1	Peristiwa mencurigakan diidentifikasi dan ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-resource-check	Pastikan bahwa jenis sumber daya memiliki CloudWatch alarm untuk metrik bernama. Untuk jenis sumber daya, Anda dapat menentukan volume EBS, EC2 instans, kluster Amazon RDS, atau bucket S3. Aturannya SESUAI jika metrik bernama memiliki ID sumber daya dan CloudWatch alarm.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.5.1	Peristiwa mencurigakan diidentifikasi dan ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-settings-check	Pastikan CloudWatch alarm dengan nama metrik yang diberikan memiliki pengaturan yang ditentukan.
A3.5.1	Peristiwa mencurigakan diidentifikasi dan ditanggapi. (PCI-DSS-V4.0)	wafv2- rulegroup-logging-enabled	Pastikan pengumpulan metrik CloudWatch keamanan Amazon pada grup AWS WAFv2 aturan diaktifkan. Aturannya adalah NON_COMPLIANT jika '. VisibilityConfig CloudWatchMetricsEnabled'bidang disetel ke false.
A3.5.1	Peristiwa mencurigakan diidentifikasi dan ditanggapi. (PCI-DSS-V4.0)	sns-topic-message-delivery-notifikasi-diaktifkan	Pastikan pencatatan Amazon Simple Notification Service (SNS) diaktifkan untuk status pengiriman pesan notifikasi yang dikirim ke topik untuk titik akhir. Aturannya adalah NON_COMPLIANT jika pemberitahuan status pengiriman untuk pesan tidak diaktifkan.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk PCI DSS 4.0 (Tidak termasuk jenis sumber daya global).

Praktik Terbaik Operasional untuk PCI DSS 4.0 (Termasuk jenis sumber daya global)

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini menyediakan contoh pemetaan antara Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) 4.0 (Tidak termasuk tipe sumber daya global) dan aturan Config terkelola AWS . Setiap AWS Config aturan berlaku untuk AWS sumber daya tertentu, dan berhubungan dengan satu atau lebih kontrol PCI DSS. Kontrol PCI DSS dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.2.5	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	cloudfront-security-policy-check	Pastikan CloudFront distribusi Amazon menggunakan kebijakan keamanan minimum dan rangkaian sandi TLSv1 0,2 atau lebih tinggi untuk koneksi penampil. Aturan ini adalah NON_COMPLIANT untuk CloudFront distribusi jika di bawah .2_2018

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			minimumProtocolVersion . TLSv1
1.2.5	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	cloudfront-sni-enabled	Pastikan CloudFront distribusi Amazon menggunakan sertifikat SSL khusus dan dikonfigurasi untuk menggunakan SNI untuk melayani permintaan HTTPS. Aturannya adalah NON_COMPLIANT jika sertifikat SSL khusus dikaitkan tetapi metode dukungan SSL adalah alamat IP khusus.
1.2.5	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	transfer-family-server-no-ftp	Pastikan server yang dibuat dengan AWS Transfer Family tidak menggunakan FTP untuk koneksi endpoint. Aturannya adalah NON_COMPLIANT jika protokol server untuk koneksi endpoint diaktifkan FTP.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.2.5	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	cloudfront-no-deprecated-ssl-protokol	Pastikan CloudFront distribusi tidak menggunakan protokol SSL yang tidak digunakan lagi untuk komunikasi HTTPS antara lokasi tepi dan asal kustom. CloudFront Aturan ini adalah NON_COMPLIANT untuk CloudFront distribusi jika ada 'termasuk'. OriginSslProtocols SSLv3
1.2.5	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	cloudfront-traffic-to-origin-dienkripsi	Pastikan CloudFront distribusi Amazon mengenkripsi lalu lintas ke asal kustom. Aturannya adalah NON_COMPLIANT jika '' is'http-only' atau jika' 'adalah OriginProtocolPolicy 'match-viewer' dan' 'allow-all'. OriginProtocolPolicy ViewerProtocolPolicy

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.2.5	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	cloudfront-viewer-policy-https	Pastikan CloudFront distribusi Amazon Anda menggunakan HTTPS (secara langsung atau melalui pengalihan). Aturannya adalah NON_COMPLIANT jika nilai ViewerProtocolPolicy disetel ke 'allow-all' untuk atau untuk. DefaultCacheBehavior CacheBehaviors
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	api-gw-endpoint-type-periksa	Pastikan bahwa Amazon API Gateway APIs adalah tipe yang ditentukan dalam parameter aturan 'endpointConfigurationType'. Aturan mengembalikan NON_COMPLIANT jika REST API tidak cocok dengan tipe titik akhir yang dikonfigurasi dalam parameter aturan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	cloudfront-associated-with-waf	Pastikan CloudFront distribusi Amazon dikaitkan dengan firewall aplikasi web (WAF) atau daftar kontrol akses WAFv2 web (ACLs). Aturannya adalah NON_COMPLIANT jika CloudFront distribusi tidak terkait dengan ACL web WAF.
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	cloudfront-custom-ssl-certificate	Pastikan sertifikat yang terkait dengan CloudFront distribusi Amazon bukan sertifikat SSL default. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi menggunakan sertifikat SSL default.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	netfw-policy-default-action-fragmen-paket	Pastikan kebijakan AWS Network Firewall dikonfigurasi dengan tindakan default stateless yang ditentukan pengguna untuk paket terfragmentasi. Aturannya adalah NON_COMPLIANT jika tindakan default stateless untuk paket terfragmentasi tidak cocok dengan tindakan default yang ditentukan pengguna.
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	rds-db-security-group-tidak diizinkan	Pastikan bahwa grup keamanan Amazon Relational Database Service (Amazon RDS) DB adalah yang default. Aturannya adalah NON_COMPLIANT jika ada grup keamanan DB yang bukan grup keamanan DB default.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan	Pastikan Gateway Transit Amazon Elastic Compute Cloud (Amazon EC2) tidak mengaktifkan "AutoAcceptSharedAttachments. Aturannya adalah NON_COMPLIANT untuk Transit Gateway jika " disetel ke AutoAcceptSharedAttachments 'aktifkan'.
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	eks-endpoint-no-public-akses	Pastikan titik akhir Amazon Elastic Kubernetes Service (Amazon EKS) tidak dapat diakses publik. Aturannya adalah NON_COMPLIANT jika titik akhir dapat diakses publik.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	terbatas-ssh	Catatan: Untuk aturan ini, pengidentifikasi aturan (INCOMING _SSH_DISABLED) dan nama aturan (restricted-ssh) berbeda. Pastikan bahwa lalu lintas SSH yang masuk untuk grup keamanan dapat diakses. Aturannya adalah COMPLIANT jika alamat IP dari lalu lintas SSH yang masuk dalam grup keamanan dibatasi (CIDR selain 0.0.0.0/0 atau: :/0). Jika tidak, NON_COMPLIANT.
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	appsync-associated-with-waf	Pastikan AWS AppSync APIs yang terkait dengan daftar kontrol akses AWS WAFv2 web (ACLs). Aturannya adalah NON_COMPLIANT untuk AWS AppSync API jika tidak terkait dengan ACL web.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	docdb-cluster-snapshot-public-dilarang	Pastikan snapshot cluster manual Amazon DocumentDB tidak bersifat publik. Aturannya adalah NON_COMPLIANT jika ada snapshot cluster manual Amazon DocumentDB yang bersifat publik.
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber Bitbucket TIDAK berisi kredenal masuk atau tidak. Aturannya adalah NON_COMPLIANT jika URL berisi informasi login dan COMPLIANT jika tidak.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	emr-block-public-access	Pastikan akun dengan Amazon EMR telah mengaktifkan pengaturan akses publik yang memblokir. Aturannya adalah NON_COMPLIANT jika BlockPublicSecurityGroupRules salah, atau jika benar, port selain Port 22 terdaftar di. PermittedPublicSecurityGroupRuleRanges
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	nacl-no-unrestricted-ssh-rdp	Pastikan port default untuk lalu lintas masuk SSH/RDP untuk daftar kontrol akses jaringan () dibatasi. NACLs Aturannya adalah NON_COMPLIANT jika entri masuk NACL memungkinkan blok sumber TCP atau UDP CIDR untuk port 22 atau 3389.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	waf-global-webacl-not-kosong	Pastikan bahwa WAF Global Web ACL berisi beberapa aturan WAF atau grup aturan. Aturan ini adalah NON_COMPLIANT jika ACL Web tidak berisi aturan WAF atau grup aturan.
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	waf-global-rulegroup-not-kosong	Pastikan grup aturan AWS WAF Classic berisi beberapa aturan. Aturannya adalah NON_COMPLIANT jika tidak ada aturan yang ada dalam grup aturan.
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	waf-global-rule-not-kosong	Pastikan bahwa aturan global AWS WAF berisi beberapa kondisi. Aturannya adalah NON_COMPLIANT jika tidak ada kondisi dalam aturan global WAF.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	ec2- -semua client-vpn-not-authorize	Pastikan bahwa aturan otorisasi AWS Client VPN tidak mengotorisasi akses koneksi untuk semua klien. Aturannya adalah NON_COMPLIANT jika 'AccessAll' hadir dan disetel ke true.
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	internet-gateway-authorized-vpc-hanya	Pastikan gateway internet dilampirkan ke cloud pribadi virtual resmi (Amazon VPC). Aturannya adalah NON_COMPLIANT jika gateway internet dilampirkan ke VPC yang tidak sah.
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	s3- -blok access-point-public-access	Pastikan jalur akses Amazon S3 telah mengaktifkan pengaturan akses publik blokir. Aturannya adalah NON_COMPLIANT jika pengaturan akses publik blok tidak diaktifkan untuk titik akses S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.2.8	Kontrol keamanan jaringan (NSCs) dikonfigurasi dan dipelihara. (PCI-DSS-V4.0)	s3- -blok account-level-public-access	Pastikan bahwa pengaturan blok akses publik yang diperlukan dikonfigurasi dari tingkat akun. Aturannya hanya NON_COMPLIANT jika bidang yang ditetapkan di bawah ini tidak cocok dengan bidang yang sesuai di item konfigurasi.
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	api-gw-endpoint-type-periksa	Pastikan bahwa Amazon API Gateway APIs adalah tipe yang ditentukan dalam parameter aturan 'endpointConfigurationType'. Aturan mengembalikan NON_COMPLIANT jika REST API tidak cocok dengan tipe titik akhir yang dikonfigurasi dalam parameter aturan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	cloudfront-associated-with-waf	Pastikan CloudFront distribusi Amazon dikaitkan dengan firewall aplikasi web (WAF) atau daftar kontrol akses WAFv2 web (ACLs). Aturannya adalah NON_COMPLIANT jika CloudFront distribusi tidak terkait dengan ACL web WAF.
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	cloudfront-custom-ssl-certificate	Pastikan sertifikat yang terkait dengan CloudFront distribusi Amazon bukan sertifikat SSL default. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi menggunakan sertifikat SSL default.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	netfw-policy-default-action-fragmen-paket	Pastikan kebijakan AWS Network Firewall dikonfigurasi dengan tindakan default stateless yang ditentukan pengguna untuk paket terfragmentasi. Aturannya adalah NON_COMPLIANT jika tindakan default stateless untuk paket terfragmentasi tidak cocok dengan tindakan default yang ditentukan pengguna.
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	rds-db-security-group-tidak diizinkan	Pastikan bahwa grup keamanan Amazon Relational Database Service (Amazon RDS) DB adalah yang default. Aturannya adalah NON_COMPLIANT jika ada grup keamanan DB yang bukan grup keamanan DB default.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	redshift-enhanced-vpc-routing-diaktifkan	Pastikan bahwa klaster Amazon Redshift telah 'diaktifkan. enhancedVpcRouting Aturannya adalah NON_COMPLIANT jika 'enhanced VpcRouting' tidak diaktifkan atau jika konfigurasi. enhancedVpcRouting lapangan adalah 'palsu'.
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan	Pastikan Gateway Transit Amazon Elastic Compute Cloud (Amazon EC2) tidak mengaktifkan "AutoAcceptSharedAttachments. Aturannya adalah NON_COMPLIANT untuk Transit Gateway jika " disetel ke AutoAcceptSharedAttachments 'aktifkan'.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	eks-endpoint-no-public-akses	Pastikan titik akhir Amazon Elastic Kubernetes Service (Amazon EKS) tidak dapat diakses publik. Aturannya adalah NON_COMPLIANT jika titik akhir dapat diakses publik.
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	terbatas-ssh	Catatan: Untuk aturan ini, pengidentifikasi aturan (INCOMING_SSH_DISABLED) dan nama aturan (restricted-ssh) berbeda. Pastikan bahwa lalu lintas SSH yang masuk untuk grup keamanan dapat diakses. Aturannya adalah COMPLIANT jika alamat IP dari lalu lintas SSH yang masuk dalam grup keamanan dibatasi (CIDR selain 0.0.0.0/0 atau: :/0). Jika tidak, NON_COMPLIANT.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	appsync-associated-with-waf	Pastikan AWS AppSync APIs yang terkait dengan daftar kontrol akses AWS WAFv2 web (ACLs). Aturannya adalah NON_COMPLIANT untuk AWS AppSync API jika tidak terkait dengan ACL web.
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	docdb-cluster-snapshot-public-dilarang	Pastikan snapshot cluster manual Amazon DocumentDB tidak bersifat publik. Aturannya adalah NON_COMPLIANT jika ada snapshot cluster manual Amazon DocumentDB yang bersifat publik.
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber Bitbucket TIDAK berisi kredenal masuk atau tidak. Aturannya adalah NON_COMPLIANT jika URL berisi informasi login dan COMPLIANT jika tidak.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	emr-block-public-access	Pastikan akun dengan Amazon EMR telah mengaktifkan pengaturan akses publik yang memblokir. Aturannya adalah NON_COMPLIANT jika BlockPublicSecurityGroupRules salah, atau jika benar, port selain Port 22 terdaftar di. PermittedPublicSecurityGroupRuleRanges
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	nacl-no-unrestricted-ssh-rdp	Pastikan port default untuk lalu lintas masuk SSH/RDP untuk daftar kontrol akses jaringan () dibatasi. NACLs Aturannya adalah NON_COMPLIANT jika entri masuk NACL memungkinkan blok sumber TCP atau UDP CIDR untuk port 22 atau 3389.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	waf-global-webacl-not-kosong	Pastikan bahwa WAF Global Web ACL berisi beberapa aturan WAF atau grup aturan. Aturan ini adalah NON_COMPLIANT jika ACL Web tidak berisi aturan WAF atau grup aturan.
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	waf-global-rulegroup-not-kosong	Pastikan grup aturan AWS WAF Classic berisi beberapa aturan. Aturannya adalah NON_COMPLIANT jika tidak ada aturan yang ada dalam grup aturan.
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	waf-global-rule-not-kosong	Pastikan bahwa aturan global AWS WAF berisi beberapa kondisi. Aturannya adalah NON_COMPLIANT jika tidak ada kondisi dalam aturan global WAF.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	ec2- -semua client-vpn-not-authorize	Pastikan bahwa aturan otorisasi AWS Client VPN tidak mengotorisasi akses koneksi untuk semua klien. Aturannya adalah NON_COMPLIANT jika 'AccessAll' hadir dan disetel ke true.
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	internet-gateway-authorized-vpc-hanya	Pastikan gateway internet dilampirkan ke cloud pribadi virtual resmi (Amazon VPC). Aturannya adalah NON_COMPLIANT jika gateway internet dilampirkan ke VPC yang tidak sah.
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	s3- -blok access-point-public-access	Pastikan jalur akses Amazon S3 telah mengaktifkan pengaturan akses publik blokir. Aturannya adalah NON_COMPLIANT jika pengaturan akses publik blok tidak diaktifkan untuk titik akses S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.1	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	s3- -blok account-level-public-access	Pastikan bahwa pengaturan blok akses publik yang diperlukan dikonfigurasi dari tingkat akun. Aturannya hanya NON_COMPLIANT jika bidang yang ditetapkan di bawah ini tidak cocok dengan bidang yang sesuai di item konfigurasi.
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	api-gw-endpoint-type-periksa	Pastikan bahwa Amazon API Gateway APIs adalah tipe yang ditentukan dalam parameter aturan 'endpointConfigurationType'. Aturan mengembalikan NON_COMPLIANT jika REST API tidak cocok dengan tipe titik akhir yang dikonfigurasi dalam parameter aturan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	cloudfront-associated-with-waf	Pastikan CloudFront distribusi Amazon dikaitkan dengan firewall aplikasi web (WAF) atau daftar kontrol akses WAFv2 web (ACLs). Aturannya adalah NON_COMPLIANT jika CloudFront distribusi tidak terkait dengan ACL web WAF.
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	cloudfront-custom-ssl-certificate	Pastikan sertifikat yang terkait dengan CloudFront distribusi Amazon bukan sertifikat SSL default. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi menggunakan sertifikat SSL default.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	netfw-policy-default-action-fragmen-paket	Pastikan kebijakan AWS Network Firewall dikonfigurasi dengan tindakan default stateless yang ditentukan pengguna untuk paket terfragmentasi. Aturannya adalah NON_COMPLIANT jika tindakan default stateless untuk paket terfragmentasi tidak cocok dengan tindakan default yang ditentukan pengguna.
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	rds-db-security-group-tidak diizinkan	Pastikan bahwa grup keamanan Amazon Relational Database Service (Amazon RDS) DB adalah yang default. Aturannya adalah NON_COMPLIANT jika ada grup keamanan DB yang bukan grup keamanan DB default.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	redshift-enhanced-vpc-routing-diaktifkan	Pastikan bahwa klaster Amazon Redshift telah 'diaktifkan. enhancedVpcRouting Aturannya adalah NON_COMPLIANT jika 'enhancedVpcRouting' tidak diaktifkan atau jika konfigurasi. enhancedVpcRouting lapangan adalah 'palsu'.
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan	Pastikan Gateway Transit Amazon Elastic Compute Cloud (Amazon EC2) tidak mengaktifkan "AutoAcceptSharedAttachments. Aturannya adalah NON_COMPLIANT untuk Transit Gateway jika " disetel ke AutoAcceptSharedAttachments 'aktifkan'.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	eks-endpoint-no-public-akses	Pastikan titik akhir Amazon Elastic Kubernetes Service (Amazon EKS) tidak dapat diakses publik. Aturannya adalah NON_COMPLIANT jika titik akhir dapat diakses publik.
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	terbatas-ssh	Catatan: Untuk aturan ini, pengidentifikasi aturan (INCOMING_SSH_DISABLED) dan nama aturan (restricted-ssh) berbeda. Pastikan bahwa lalu lintas SSH yang masuk untuk grup keamanan dapat diakses. Aturannya adalah COMPLIANT jika alamat IP dari lalu lintas SSH yang masuk dalam grup keamanan dibatasi (CIDR selain 0.0.0.0/0 atau: :/0). Jika tidak, NON_COMPLIANT.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	appsync-associated-with-waf	Pastikan AWS AppSync APIs yang terkait dengan daftar kontrol akses AWS WAFv2 web (ACLs). Aturannya adalah NON_COMPLIANT untuk AWS AppSync API jika tidak terkait dengan ACL web.
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	docdb-cluster-snapshot-public-dilarang	Pastikan snapshot cluster manual Amazon DocumentDB tidak bersifat publik. Aturannya adalah NON_COMPLIANT jika ada snapshot cluster manual Amazon DocumentDB yang bersifat publik.
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber Bitbucket TIDAK berisi kredenal masuk atau tidak. Aturannya adalah NON_COMPLIANT jika URL berisi informasi login dan COMPLIANT jika tidak.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	emr-block-public-access	Pastikan akun dengan Amazon EMR telah mengaktifkan pengaturan akses publik yang memblokir. Aturannya adalah NON_COMPLIANT jika BlockPublicSecurityGroupRules salah, atau jika benar, port selain Port 22 terdaftar di. PermittedPublicSecurityGroupRuleRanges
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	nacl-no-unrestricted-ssh-rdp	Pastikan port default untuk lalu lintas masuk SSH/RDP untuk daftar kontrol akses jaringan () dibatasi. NACLs Aturannya adalah NON_COMPLIANT jika entri masuk NACL memungkinkan blok sumber TCP atau UDP CIDR untuk port 22 atau 3389.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	waf-global-webacl-not-kosong	Pastikan bahwa WAF Global Web ACL berisi beberapa aturan WAF atau grup aturan. Aturan ini adalah NON_COMPLIANT jika ACL Web tidak berisi aturan WAF atau grup aturan.
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	waf-global-rulegroup-not-kosong	Pastikan grup aturan AWS WAF Classic berisi beberapa aturan. Aturannya adalah NON_COMPLIANT jika tidak ada aturan yang ada dalam grup aturan.
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	waf-global-rule-not-kosong	Pastikan bahwa aturan global AWS WAF berisi beberapa kondisi. Aturannya adalah NON_COMPLIANT jika tidak ada kondisi dalam aturan global WAF.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	ec2- -semua client-vpn-not-authorize	Pastikan bahwa aturan otorisasi AWS Client VPN tidak mengotorisasi akses koneksi untuk semua klien. Aturannya adalah NON_COMPLIANT jika 'AccessAll' hadir dan disetel ke true.
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	internet-gateway-authorized-vpc-hanya	Pastikan gateway internet dilampirkan ke cloud pribadi virtual resmi (Amazon VPC). Aturannya adalah NON_COMPLIANT jika gateway internet dilampirkan ke VPC yang tidak sah.
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	s3- -blok access-point-public-access	Pastikan jalur akses Amazon S3 telah mengaktifkan pengaturan akses publik blokir. Aturannya adalah NON_COMPLIANT jika pengaturan akses publik blok tidak diaktifkan untuk titik akses S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.3.2	Akses jaringan ke dan dari lingkungan data pemegang kartu dibatasi. (PCI-DSS-V4.0)	s3- -blok account-level-public-access	Pastikan bahwa pengaturan blok akses publik yang diperlukan dikonfigurasi dari tingkat akun. Aturannya hanya NON_COMPLIANT jika bidang yang ditetapkan di bawah ini tidak cocok dengan bidang yang sesuai di item konfigurasi.
1.4.1	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendalikan. (PCI-DSS-V4.0)	api-gw-endpoint-type-periksa	Pastikan bahwa Amazon API Gateway APIs adalah tipe yang ditentukan dalam parameter aturan 'endpointConfigurationType'. Aturan mengembalikan NON_COMPLIANT jika REST API tidak cocok dengan tipe titik akhir yang dikonfigurasi dalam parameter aturan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.1	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	redshift-enhanced-vpc-routing-diaktifkan	Pastikan bahwa klaster Amazon Redshift telah 'diaktifk an. enhancedV pcRouting Aturannya adalah NON_COMPL IANT jika 'enhanced VpcRouting' tidak diaktifkan atau jika konfigurasi. enhancedVpcRouting lapangan adalah 'palsu'.
1.4.1	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	internet-gateway-a uthorized-vpc-hanya	Pastikan gateway internet dilampirkan ke cloud pribadi virtual resmi (Amazon VPC). Aturannya adalah NON_COMPLIANT jika gateway internet dilampirkan ke VPC yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	api-gw-endpoint-type-periksa	Pastikan bahwa Amazon API Gateway APIs adalah tipe yang ditentukan dalam parameter aturan 'endpointConfigura tionType'. Aturan mengembalikan NON_COMPLIANT jika REST API tidak cocok dengan tipe titik akhir yang dikonfigu rasi dalam parameter aturan.
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	cloudfront-associated-with-waf	Pastikan CloudFron t distribusi Amazon dikaitkan dengan firewall aplikasi web (WAF) atau daftar kontrol akses WAFv2 web (ACLs). Aturannya adalah NON_COMPLIANT jika CloudFront distribusi tidak terkait dengan ACL web WAF.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	cloudfront-custom-ssl-certificate	Pastikan sertifikat yang terkait dengan CloudFront distribus i Amazon bukan sertifikat SSL default. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi menggunak an sertifikat SSL default.
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	netfw-policy-default-action-fragmen-paket	Pastikan kebijakan AWS Network Firewall dikonfigurasi dengan tindakan default stateless yang ditentukan pengguna untuk paket terfragme ntasi. Aturannya adalah NON_COMPL IANT jika tindakan default stateless untuk paket terfragmentasi tidak cocok dengan tindakan default yang ditentukan pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	rds-db-security-group-tidak diizinkan	Pastikan bahwa grup keamanan Amazon Relational Database Service (Amazon RDS) DB adalah yang default. Aturannya adalah NON_COMPL IANT jika ada grup keamanan DB yang bukan grup keamanan DB default.
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	redshift-enhanced-vpc-routing-diaktifkan	Pastikan bahwa klaster Amazon Redshift telah 'diaktifk an. enhancedV pcRouting Aturannya adalah NON_COMPL IANT jika 'enhanced VpcRouting' tidak diaktifkan atau jika konfigurasi. enhancedVpcRouting lapangan adalah 'palsu'.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan	Pastikan Gateway Transit Amazon Elastic Compute Cloud (Amazon EC2) tidak mengaktif kan "AutoAcc eptSharedAttachmen ts. Aturannya adalah NON_COMPL IANT untuk Transit Gateway jika " disetel ke AutoAccep tSharedAttachments 'aktifkan'.
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	eks-endpoint-no-pu blic-akses	Pastikan titik akhir Amazon Elastic Kubernetes Service (Amazon EKS) tidak dapat diakses publik. Aturannya adalah NON_COMPLIANT jika titik akhir dapat diakses publik.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	terbatas-ssh	Catatan: Untuk aturan ini, pengidentifikasi aturan (INCOMING _SSH_DISABLED) dan nama aturan (restricted-ssh) berbeda. Pastikan bahwa lalu lintas SSH yang masuk untuk grup keamanan dapat diakses. Aturannya adalah COMPLIANT jika alamat IP dari lalu lintas SSH yang masuk dalam grup keamanan dibatasi (CIDR selain 0.0.0.0/0 atau: :/0). Jika tidak, NON_COMPLIANT.
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	appsync-associated-with-waf	Pastikan AWS AppSync APIs yang terkait dengan daftar kontrol akses AWS WAFv2 web (ACLs). Aturannya adalah NON_COMPLIANT untuk AWS AppSync API jika tidak terkait dengan ACL web.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	docdb-cluster-snap shot-public-dilarang	Pastikan snapshot cluster manual Amazon DocumentD B tidak bersifat publik. Aturannya adalah NON_COMPLIANT jika ada snapshot cluster manual Amazon DocumentDB yang bersifat publik.
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	codebuild-project-source-repo-url-pe riksa	Pastikan URL repositori sumber Bitbucket TIDAK berisi kredenal masuk atau tidak. Aturannya adalah NON_COMPL IANT jika URL berisi informasi login dan COMPLIANT jika tidak.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunak an sertifikat SSL yang disediaka n oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Applicati on Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	emr-block-public-access	Pastikan akun dengan Amazon EMR telah mengaktif kan pengaturan akses publik yang memblokir. Aturannya adalah NON_COMPLIANT jika BlockPublicSecurityGroupRules salah, atau jika benar, port selain Port 22 terdaftar di. PermittedPublicSecurityGroupRuleRanges
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	nacl-no-unrestricted-ssh-rdp	Pastikan port default untuk lalu lintas masuk SSH/RDP untuk daftar kontrol akses jaringan () dibatasi. NACLs Aturannya adalah NON_COMPLIANT jika entri masuk NACL memungkinkan blok sumber TCP atau UDP CIDR untuk port 22 atau 3389.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	waf-global-webacl-not-kosong	Pastikan bahwa WAF Global Web ACL berisi beberapa aturan WAF atau grup aturan. Aturan ini adalah NON_COMPL IANT jika ACL Web tidak berisi aturan WAF atau grup aturan.
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	waf-global-rulegroup-not-kosong	Pastikan grup aturan AWS WAF Classic berisi beberapa aturan. Aturannya adalah NON_COMPL IANT jika tidak ada aturan yang ada dalam grup aturan.
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	waf-global-rule-not-kosong	Pastikan bahwa aturan global AWS WAF berisi beberapa kondisi. Aturannya adalah NON_COMPL IANT jika tidak ada kondisi dalam aturan global WAF.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	ec2- -semua client-vpn-not-authorize	Pastikan bahwa aturan otorisasi AWS Client VPN tidak mengotorisasi akses koneksi untuk semua klien. Aturannya adalah NON_COMPLIANT jika 'AccessAll' hadir dan disetel ke true.
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	internet-gateway-authorized-vpc-hanya	Pastikan gateway internet dilampirkan ke cloud pribadi virtual resmi (Amazon VPC). Aturannya adalah NON_COMPLIANT jika gateway internet dilampirkan ke VPC yang tidak sah.
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	s3- -blok access-point-public-access	Pastikan jalur akses Amazon S3 telah mengaktif kan pengaturan akses publik blokir. Aturannya adalah NON_COMPLIANT jika pengaturan akses publik blok tidak diaktifkan untuk titik akses S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.2	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	s3- -blok account-l evel-public-access	Pastikan bahwa pengaturan blok akses publik yang diperlukan dikonfigu rasi dari tingkat akun. Aturannya hanya NON_COMPLIANT jika bidang yang ditetapkan di bawah ini tidak cocok dengan bidang yang sesuai di item konfigurasi.
1.4.3	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	netfw-policy-default-action-fragmen-paket	Pastikan kebijakan AWS Network Firewall dikonfigurasi dengan tindakan default stateless yang ditentukan pengguna untuk paket terfragme ntasi. Aturannya adalah NON_COMPL IANT jika tindakan default stateless untuk paket terfragmentasi tidak cocok dengan tindakan default yang ditentukan pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.3	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	netfw-policy-default-action-fragmen-paket	Pastikan kebijakan AWS Network Firewall dikonfigurasi dengan tindakan default stateless yang ditentukan pengguna untuk paket terfragme ntasi. Aturannya adalah NON_COMPL IANT jika tindakan default stateless untuk paket terfragmentasi tidak cocok dengan tindakan default yang ditentukan pengguna.
1.4.3	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	netfw-policy-default-action-paket penuh	Pastikan kebijakan AWS Network Firewall dikonfigurasi dengan tindakan stateless default yang ditentuka n pengguna untuk paket lengkap. Aturan ini adalah NON_COMPLIANT jika tindakan stateless default untuk paket lengkap tidak cocok dengan tindakan stateless default yang ditentukan pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.4	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	api-gw-endpoint-type-periksa	Pastikan bahwa Amazon API Gateway APIs adalah tipe yang ditentukan dalam parameter aturan 'endpointConfigura tionType'. Aturan mengembalikan NON_COMPLIANT jika REST API tidak cocok dengan tipe titik akhir yang dikonfigu rasi dalam parameter aturan.
1.4.4	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	redshift-enhanced-vpc-routing-diaktifkan	Pastikan bahwa klaster Amazon Redshift telah 'diaktifk an. enhancedV pcRouting Aturannya adalah NON_COMPL IANT jika 'enhanced VpcRouting' tidak diaktifkan atau jika konfigurasi. enhancedVpcRouting lapangan adalah 'palsu'.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.4	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	internet-gateway-a uthorized-vpc-hanya	Pastikan gateway internet dilampirkan ke cloud pribadi virtual resmi (Amazon VPC). Aturannya adalah NON_COMPLIANT jika gateway internet dilampirkan ke VPC yang tidak sah.
1.4.5	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	ecs-task-definition-pid-mode-periksa	Pastikan bahwa ECSTask Definisi dikonfigurasi untuk berbagi namespace proses host dengan wadah Amazon Elastic Container Service (Amazon ECS). Aturannya adalah NON_COMPL IANT jika parameter PidMode disetel ke 'host'.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.4.5	Koneksi jaringan antara jaringan tepercaya dan tidak tepercaya dikendali kan. (PCI-DSS-V4.0)	ec2- launch-template-public-ip -dinonaktifkan	Pastikan Template EC2 Peluncuran Amazon tidak disetel untuk menetapkan alamat IP publik ke Antarmuka Jaringan. Aturannya adalah NON_COMPL IANT jika versi default Template EC2 Peluncuran memiliki setidaknya 1 Antarmuka Jaringan dengan '' disetel ke AssociatePublicIpA ddress 'benar'.
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	api-gw-endpoint-type-periksa	Pastikan bahwa Amazon API Gateway APIs adalah tipe yang ditentukan dalam parameter aturan 'endpointConfigura tionType'. Aturan mengembalikan NON_COMPLIANT jika REST API tidak cocok dengan tipe titik akhir yang dikonfigu rasi dalam parameter aturan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	cloudfront-associated-with-waf	Pastikan CloudFront distribusi Amazon dikaitkan dengan firewall aplikasi web (WAF) atau daftar kontrol akses WAFv2 web (ACLs). Aturannya adalah NON_COMPLIANT jika CloudFront distribusi tidak terkait dengan ACL web WAF.
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	cloudfront-custom-ssl-certificate	Pastikan sertifikat yang terkait dengan CloudFront distribusi Amazon bukan sertifikat SSL default. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi menggunakan sertifikat SSL default.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	netfw-policy-default-action-fragmen-paket	Pastikan kebijakan AWS Network Firewall dikonfigurasi dengan tindakan default stateless yang ditentukan pengguna untuk paket terfragmentasi. Aturannya adalah NON_COMPLIANT jika tindakan default stateless untuk paket terfragmentasi tidak cocok dengan tindakan default yang ditentukan pengguna.
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	rds-db-security-group-tidak diizinkan	Pastikan bahwa grup keamanan Amazon Relational Database Service (Amazon RDS) DB adalah yang default. Aturannya adalah NON_COMPLIANT jika ada grup keamanan DB yang bukan grup keamanan DB default.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan	Pastikan Gateway Transit Amazon Elastic Compute Cloud (Amazon EC2) tidak mengaktifkan "AutoAcceptSharedAttachments. Aturannya adalah NON_COMPLIANT untuk Transit Gateway jika " disetel ke AutoAcceptSharedAttachments 'aktifkan'.
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	eks-endpoint-no-public-akses	Pastikan titik akhir Amazon Elastic Kubernetes Service (Amazon EKS) tidak dapat diakses publik. Aturannya adalah NON_COMPLIANT jika titik akhir dapat diakses publik.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	terbatas-ssh	Catatan: Untuk aturan ini, pengidentifikasi aturan (INCOMING _SSH_DISABLED) dan nama aturan (restricted-ssh) berbeda. Pastikan bahwa lalu lintas SSH yang masuk untuk grup keamanan dapat diakses. Aturannya adalah COMPLIANT jika alamat IP dari lalu lintas SSH yang masuk dalam grup keamanan dibatasi (CIDR selain 0.0.0.0/0 atau: :/0). Jika tidak, NON_COMPLIANT.
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	appsync-associated-with-waf	Pastikan AWS AppSync APIs yang terkait dengan daftar kontrol akses AWS WAFv2 web (ACLs). Aturannya adalah NON_COMPLIANT untuk AWS AppSync API jika tidak terkait dengan ACL web.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	docdb-cluster-snapshot-public-dilarang	Pastikan snapshot cluster manual Amazon DocumentDB tidak bersifat publik. Aturannya adalah NON_COMPLIANT jika ada snapshot cluster manual Amazon DocumentDB yang bersifat publik.
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber Bitbucket TIDAK berisi kredenal masuk atau tidak. Aturannya adalah NON_COMPLIANT jika URL berisi informasi login dan COMPLIANT jika tidak.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	emr-block-public-access	Pastikan akun dengan Amazon EMR telah mengaktifkan pengaturan akses publik yang memblokir. Aturannya adalah NON_COMPLIANT jika BlockPublicSecurityGroupRules salah, atau jika benar, port selain Port 22 terdaftar di. PermittedPublicSecurityGroupRuleRanges
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	nacl-no-unrestricted-ssh-rdp	Pastikan port default untuk lalu lintas masuk SSH/RDP untuk daftar kontrol akses jaringan () dibatasi. NACLs Aturannya adalah NON_COMPLIANT jika entri masuk NACL memungkinkan blok sumber TCP atau UDP CIDR untuk port 22 atau 3389.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	waf-global-webacl-not-kosong	Pastikan bahwa WAF Global Web ACL berisi beberapa aturan WAF atau grup aturan. Aturan ini adalah NON_COMPLIANT jika ACL Web tidak berisi aturan WAF atau grup aturan.
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	waf-global-rulegroup-not-kosong	Pastikan grup aturan AWS WAF Classic berisi beberapa aturan. Aturannya adalah NON_COMPLIANT jika tidak ada aturan yang ada dalam grup aturan.
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	waf-global-rule-not-kosong	Pastikan bahwa aturan global AWS WAF berisi beberapa kondisi. Aturannya adalah NON_COMPLIANT jika tidak ada kondisi dalam aturan global WAF.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	ec2- -semua client-vpn-not-authorize	Pastikan bahwa aturan otorisasi AWS Client VPN tidak mengotorisasi akses koneksi untuk semua klien. Aturannya adalah NON_COMPLIANT jika 'AccessAll' hadir dan disetel ke true.
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	internet-gateway-authorized-vpc-hanya	Pastikan gateway internet dilampirkan ke cloud pribadi virtual resmi (Amazon VPC). Aturannya adalah NON_COMPLIANT jika gateway internet dilampirkan ke VPC yang tidak sah.
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	s3- -blok access-point-public-access	Pastikan jalur akses Amazon S3 telah mengaktifkan pengaturan akses publik blokir. Aturannya adalah NON_COMPLIANT jika pengaturan akses publik blok tidak diaktifkan untuk titik akses S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
1.5.1	Risiko terhadap CDE dari perangkat komputasi yang dapat terhubung ke jaringan yang tidak tepercaya dan CDE dikurangi. (PCI-DSS-V4.0)	s3- -blok account-level-public-access	Pastikan bahwa pengaturan blok akses publik yang diperlukan dikonfigurasi dari tingkat akun. Aturannya hanya NON_COMPLIANT jika bidang yang ditetapkan di bawah ini tidak cocok dengan bidang yang sesuai di item konfigurasi.
10.2.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gwv2- access-logs-enabled	Pastikan bahwa tahap Amazon API Gateway V2 mengaktifkan pencatatan akses. Aturannya adalah NON_COMPLIANT jika 'accessLogSettings' tidak ada dalam konfigurasi Stage.
10.2.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudfront-accesslogs-enabled	Pastikan CloudFront distribusi Amazon dikonfigurasi untuk mengirimkan log akses ke bucket Amazon S3. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi tidak memiliki logging yang dikonfigurasi.
10.2.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	neptune-cluster-cloudwatch-log-ekspor diaktifkan	Pastikan klaster CloudWatch Amazon Neptunus mengaktifkan ekspor log untuk log audit. Aturannya adalah NON_COMPLIANT jika cluster Neptunus tidak mengaktifkan ekspor log untuk log audit. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	ecs-task-definition-log-konfigurasi	Pastikan bahwa LogConfiguration diatur pada Definisi Tugas ECS aktif. Aturan ini NON_COMPLIANT jika ECSTask Definisi aktif tidak memiliki sumber daya LogConfiguration yang ditentukan atau nilai untuk LogConfiguration adalah null dalam setidaknya satu definisi kontainer.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudtrail-diaktifkan	Catatan: Untuk aturan ini, pengidentifikasi aturan (CLOUD_TRAIL_ENABLED) dan nama aturan (cloudtrail-enabled) berbeda. Pastikan AWS CloudTrail jejak diaktifkan di AWS akun Anda. Aturannya adalah NON_COMPLIANT jika jejak tidak diaktifkan. Secara opsional, aturan memeriksa bucket S3 tertentu, topik Amazon Simple Notification Service (Amazon SNS), dan grup log. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	multi-region-cloudtrail-enabled	Catatan: untuk aturan ini, pengidentifikasi aturan (MULTI_REGION_CLOUD_TRAIL_ENABLED) dan nama aturan () berbeda. multi-region-cloudtrail-enabled Pastikan setidaknya ada satu multi-wilayah AWS CloudTrail. Aturannya adalah NON_COMPLIANT jika jejak tidak cocok dengan parameter input. Aturannya adalah NON_COMPLIANT jika ExcludeManagementEventSources bidang tidak kosong atau jika AWS CloudTrail dikonfigurasi untuk mengecualikan peristiwa manajemen seperti peristiwa AWS KMS atau peristiwa API Data Amazon RDS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	appsync-logging-enabled	Pastikan bahwa AWS AppSync API telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan, atau 'fieldLogLevel' bukan ERROR atau SEMUA.
10.2.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	waf-classic-logging-enabled	Pastikan pencatatan diaktifkan pada daftar kontrol akses web global klasik AWS WAF (web ACLs). Aturannya adalah NON_COMPLIANT untuk ACL web global, jika tidak mengaktifkan logging.
10.2.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-logging-diaktifkan	Pastikan pialang Amazon MQ mengaktifkan pencatatan CloudWatch audit Amazon. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1	Log audit diimpleme ntasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-log-diaktifkan	Pastikan bahwa broker Amazon MQ mengaktif kan pencatatan CloudWatch audit. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.
10.2.1	Log audit diimpleme ntasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	eks-cluster-logging-enabled	Pastikan klaster Amazon Elastic Kubernetes Service (Amazon EKS) dikonfigurasi dengan logging diaktifkan. Aturannya adalah NON_COMPLIANT jika logging untuk klaster Amazon EKS tidak diaktifkan untuk semua jenis log.
10.2.1	Log audit diimpleme ntasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	elastic-beanstalk-logs-to-jam tangan awan	Pastikan lingkunga n AWS Elastic Beanstalk dikonfigu rasi untuk mengirim log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika nilai `StreamLogs` salah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	step-functions-state-machine-logging-diaktifkan	Pastikan bahwa mesin AWS Step Functions telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika mesin status tidak mengaktifkan logging atau konfigurasi logging tidak pada tingkat minimum yang disediakan.
10.2.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	netfw-logging-enabled	Pastikan firewall AWS Network Firewall telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika jenis logging tidak dikonfigurasi. Anda dapat menentukan jenis logging yang Anda ingin aturan untuk memeriksa.
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gwv2- access-logs-enabled	Pastikan bahwa tahap Amazon API Gateway V2 mengaktifkan pencatatan akses. Aturannya adalah NON_COMPLIANT jika 'accessLogSettings' tidak ada dalam konfigurasi Stage.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudfront-accesslogs-enabled	Pastikan CloudFront distribusi Amazon dikonfigurasi untuk mengirimkan log akses ke bucket Amazon S3. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi tidak memiliki logging yang dikonfigurasi.
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	neptune-cluster-cloudwatch-log-ekspor diaktifkan	Pastikan klaster CloudWatch Amazon Neptunus mengaktifkan ekspor log untuk log audit. Aturannya adalah NON_COMPLIANT jika cluster Neptunus tidak mengaktifkan ekspor log untuk log audit. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	ec2- instance-detailed-monitoring-enabled	Pastikan pemantauan terperinci diaktifkan untuk EC2 instans. Aturannya adalah NON_COMPLIANT jika pemantauan terperinci tidak diaktifkan.
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	ecs-task-definition-log-konfigurasi	Pastikan bahwa LogConfiguration diatur pada Definisi Tugas ECS aktif. Aturan ini NON_COMPLIANT jika ECSTask Definisi aktif tidak memiliki sumber daya LogConfiguration yang ditentukan atau nilai untuk LogConfiguration adalah null dalam setidaknya satu definisi kontainer.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudwatch-alarm-resource-check	Pastikan bahwa jenis sumber daya memiliki CloudWatch alarm untuk metrik bernama. Untuk jenis sumber daya, Anda dapat menentukan volume EBS, EC2 instans, kluster Amazon RDS, atau bucket S3. Aturannya adalah COMPLIANT jika metrik bernama memiliki ID sumber daya dan CloudWatch alarm.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudtrail-diaktifkan	Catatan: Untuk aturan ini, pengidentifikasi aturan (CLOUD_TRAIL_ENABLED) dan nama aturan (cloudtrail-enabled) berbeda. Pastikan AWS CloudTrail jejak diaktifkan di AWS akun Anda. Aturannya adalah NON_COMPLIANT jika jejak tidak diaktifkan. Secara opsional, aturan memeriksa bucket S3 tertentu, topik Amazon Simple Notification Service (Amazon SNS), dan grup log. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	multi-region-cloudtrail-enabled	Catatan: untuk aturan ini, pengidentifikasi aturan (MULTI_REGION_CLOUD_TRAIL_ENABLED) dan nama aturan () berbeda. multi-region-cloudtrail-enabled Pastikan setidaknya ada satu multi-wilayah AWS CloudTrail. Aturannya adalah NON_COMPLIANT jika jejak tidak cocok dengan parameter input. Aturannya adalah NON_COMPLIANT jika ExcludeManagementEventSources bidang tidak kosong atau jika AWS CloudTrail dikonfigurasi untuk mengecualikan peristiwa manajemen seperti peristiwa AWS KMS atau peristiwa API Data Amazon RDS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	appsync-logging-enabled	Pastikan bahwa AWS AppSync API telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan, atau 'fieldLogLevel' bukan ERROR atau SEMUA.
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	waf-classic-logging-enabled	Pastikan pencatatan diaktifkan pada daftar kontrol akses web global klasik AWS WAF (web ACLs). Aturannya adalah NON_COMPLIANT untuk ACL web global, jika tidak mengaktifkan logging.
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-logging-diaktifkan	Pastikan pialang Amazon MQ mengaktifkan pencatatan CloudWatch audit Amazon. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.1	Log audit diimpleme ntasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-log-diaktifkan	Pastikan bahwa broker Amazon MQ mengaktif kan pencatatan CloudWatch audit. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.
10.2.1.1	Log audit diimpleme ntasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	eks-cluster-logging-enabled	Pastikan klaster Amazon Elastic Kubernetes Service (Amazon EKS) dikonfigurasi dengan logging diaktifkan. Aturannya adalah NON_COMPLIANT jika logging untuk klaster Amazon EKS tidak diaktifkan untuk semua jenis log.
10.2.1.1	Log audit diimpleme ntasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	elastic-beanstalk-logs-to-jam tangan awan	Pastikan lingkunga n AWS Elastic Beanstalk dikonfigu rasi untuk mengirim log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika nilai `StreamLogs` salah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	wafv2- rulegroup-logging-enabled	Pastikan pengumpulan metrik CloudWatch keamanan Amazon pada grup AWS WAFv2 aturan diaktifkan. Aturannya adalah NON_COMPLIANT jika '. VisibilityConfig CloudWatchMetricsEnabled'bidang disetel ke false.
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	sns-topic-message-delivery-notifikasi-diaktifkan	Pastikan pencatatan Amazon Simple Notification Service (SNS) diaktifkan untuk status pengiriman pesan notifikasi yang dikirim ke topik untuk titik akhir. Aturannya adalah NON_COMPLIANT jika pemberitahuan status pengiriman untuk pesan tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	step-functions-state-machine-logging-diaktifkan	Pastikan bahwa mesin AWS Step Functions telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika mesin status tidak mengaktifkan logging atau konfigurasi logging tidak pada tingkat minimum yang disediakan.
10.2.1.1	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	netfw-logging-enabled	Pastikan firewall AWS Network Firewall telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika jenis logging tidak dikonfigurasi. Anda dapat menentukan jenis logging yang Anda ingin aturan untuk memeriksa.
10.2.1.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gwv2- access-logs-enabled	Pastikan bahwa tahap Amazon API Gateway V2 mengaktifkan pencatatan akses. Aturannya adalah NON_COMPLIANT jika 'accessLogSettings' tidak ada dalam konfigurasi Stage.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
10.2.1.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudfront-accesslogs-enabled	Pastikan CloudFront distribusi Amazon dikonfigurasi untuk mengirimkan log akses ke bucket Amazon S3. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi tidak memiliki logging yang dikonfigurasi.
10.2.1.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	neptune-cluster-cloudwatch-log-ekspor diaktifkan	Pastikan klaster CloudWatch Amazon Neptunus mengaktifkan ekspor log untuk log audit. Aturannya adalah NON_COMPLIANT jika cluster Neptunus tidak mengaktifkan ekspor log untuk log audit. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	ecs-task-definition-log-konfigurasi	Pastikan bahwa LogConfiguration diatur pada Definisi Tugas ECS aktif. Aturan ini NON_COMPLIANT jika ECSTask Definisi aktif tidak memiliki sumber daya LogConfiguration yang ditentukan atau nilai untuk LogConfiguration adalah null dalam setidaknya satu definisi kontainer.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudtrail-diaktifkan	Catatan: Untuk aturan ini, pengidentifikasi aturan (CLOUD_TRAIL_ENABLED) dan nama aturan (cloudtrail-enabled) berbeda. Pastikan AWS CloudTrail jejak diaktifkan di AWS akun Anda. Aturannya adalah NON_COMPLIANT jika jejak tidak diaktifkan. Secara opsional, aturan memeriksa bucket S3 tertentu, topik Amazon Simple Notification Service (Amazon SNS), dan grup log. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	multi-region-cloudtrail-enabled	Catatan: untuk aturan ini, pengidentifikasi aturan (MULTI_REGION_CLOUD_TRAIL_ENABLED) dan nama aturan () berbeda. multi-region-cloudtrail-enabled Pastikan setidaknya ada satu multi-wilayah AWS CloudTrail. Aturannya adalah NON_COMPLIANT jika jejak tidak cocok dengan parameter input. Aturannya adalah NON_COMPLIANT jika ExcludeManagementEventSources bidang tidak kosong atau jika AWS CloudTrail dikonfigurasi untuk mengecualikan peristiwa manajemen seperti peristiwa AWS KMS atau peristiwa API Data Amazon RDS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	appsync-logging-enabled	Pastikan bahwa AWS AppSync API telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan, atau 'fieldLogLevel' bukan ERROR atau SEMUA.
10.2.1.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	waf-classic-logging-enabled	Pastikan pencatatan diaktifkan pada daftar kontrol akses web global klasik AWS WAF (web ACLs). Aturannya adalah NON_COMPLIANT untuk ACL web global, jika tidak mengaktifkan logging.
10.2.1.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-logging-diaktifkan	Pastikan pialang Amazon MQ mengaktifkan pencatatan CloudWatch audit Amazon. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.2	Log audit diimpleme ntasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-log-diaktifkan	Pastikan bahwa broker Amazon MQ mengaktif kan pencatatan CloudWatch audit. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.
10.2.1.2	Log audit diimpleme ntasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	eks-cluster-logging-enabled	Pastikan klaster Amazon Elastic Kubernetes Service (Amazon EKS) dikonfigurasi dengan logging diaktifkan. Aturannya adalah NON_COMPLIANT jika logging untuk klaster Amazon EKS tidak diaktifkan untuk semua jenis log.
10.2.1.2	Log audit diimpleme ntasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	elastic-beanstalk-logs-to-jam tangan awan	Pastikan lingkunga n AWS Elastic Beanstalk dikonfigu rasi untuk mengirim log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika nilai `StreamLogs` salah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	step-functions-state-machine-logging-diaktifkan	Pastikan bahwa mesin AWS Step Functions telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika mesin status tidak mengaktifkan logging atau konfigurasi logging tidak pada tingkat minimum yang disediakan.
10.2.1.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	netfw-logging-enabled	Pastikan firewall AWS Network Firewall telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika jenis logging tidak dikonfigurasi. Anda dapat menentukan jenis logging yang Anda ingin aturan untuk memeriksa.
10.2.1.3	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gwv2- access-logs-enabled	Pastikan bahwa tahap Amazon API Gateway V2 mengaktifkan pencatatan akses. Aturannya adalah NON_COMPLIANT jika 'accessLogSettings' tidak ada dalam konfigurasi Stage.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.3	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
10.2.1.3	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudfront-accesslogs-enabled	Pastikan CloudFront distribusi Amazon dikonfigurasi untuk mengirimkan log akses ke bucket Amazon S3. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi tidak memiliki logging yang dikonfigurasi.
10.2.1.3	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	neptune-cluster-cloudwatch-log-ekspor diaktifkan	Pastikan klaster CloudWatch Amazon Neptunus mengaktifkan ekspor log untuk log audit. Aturannya adalah NON_COMPLIANT jika cluster Neptunus tidak mengaktifkan ekspor log untuk log audit. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.3	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	ecs-task-definition-log-konfigurasi	Pastikan bahwa LogConfiguration diatur pada Definisi Tugas ECS aktif. Aturan ini NON_COMPLIANT jika ECSTask Definisi aktif tidak memiliki sumber daya LogConfiguration yang ditentukan atau nilai untuk LogConfiguration adalah null dalam setidaknya satu definisi kontainer.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.3	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudtrail-diaktifkan	Catatan: Untuk aturan ini, pengidentifikasi aturan (CLOUD_TRAIL_ENABLED) dan nama aturan (cloudtrail-enabled) berbeda. Pastikan AWS CloudTrail jejak diaktifkan di AWS akun Anda. Aturannya adalah NON_COMPLIANT jika jejak tidak diaktifkan. Secara opsional, aturan memeriksa bucket S3 tertentu, topik Amazon Simple Notification Service (Amazon SNS), dan grup log. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.3	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	multi-region-cloudtrail-enabled	Catatan: untuk aturan ini, pengidentifikasi aturan (MULTI_REGION_CLOUD_TRAIL_ENABLED) dan nama aturan () berbeda. multi-region-cloudtrail-enabled Pastikan setidaknya ada satu multi-wilayah AWS CloudTrail. Aturannya adalah NON_COMPLIANT jika jejak tidak cocok dengan parameter input. Aturannya adalah NON_COMPLIANT jika ExcludeManagementEventSources bidang tidak kosong atau jika AWS CloudTrail dikonfigurasi untuk mengecualikan peristiwa manajemen seperti peristiwa AWS KMS atau peristiwa API Data Amazon RDS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.3	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	appsync-logging-enabled	Pastikan bahwa AWS AppSync API telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan, atau 'fieldLogLevel' bukan ERROR atau SEMUA.
10.2.1.3	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	waf-classic-logging-enabled	Pastikan pencatatan diaktifkan pada daftar kontrol akses web global klasik AWS WAF (web ACLs). Aturannya adalah NON_COMPLIANT untuk ACL web global, jika tidak mengaktifkan logging.
10.2.1.3	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-logging-diaktifkan	Pastikan pialang Amazon MQ mengaktifkan pencatatan CloudWatch audit Amazon. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.3	Log audit diimpleme ntasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-log-diaktifkan	Pastikan bahwa broker Amazon MQ mengaktif kan pencatatan CloudWatch audit. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.
10.2.1.3	Log audit diimpleme ntasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	eks-cluster-logging-enabled	Pastikan klaster Amazon Elastic Kubernetes Service (Amazon EKS) dikonfigurasi dengan logging diaktifkan. Aturannya adalah NON_COMPLIANT jika logging untuk klaster Amazon EKS tidak diaktifkan untuk semua jenis log.
10.2.1.3	Log audit diimpleme ntasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	elastic-beanstalk-logs-to-jam tangan awan	Pastikan lingkunga n AWS Elastic Beanstalk dikonfigu rasi untuk mengirim log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika nilai `StreamLogs` salah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.3	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	step-functions-state-machine-logging-diaktifkan	Pastikan bahwa mesin AWS Step Functions telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika mesin status tidak mengaktifkan logging atau konfigurasi logging tidak pada tingkat minimum yang disediakan.
10.2.1.3	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	netfw-logging-enabled	Pastikan firewall AWS Network Firewall telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika jenis logging tidak dikonfigurasi. Anda dapat menentukan jenis logging yang Anda ingin aturan untuk memeriksa.
10.2.1.4	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gwv2- access-logs-enabled	Pastikan bahwa tahap Amazon API Gateway V2 mengaktifkan pencatatan akses. Aturannya adalah NON_COMPLIANT jika 'accessLogSettings' tidak ada dalam konfigurasi Stage.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.4	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
10.2.1.4	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudfront-accesslogs-enabled	Pastikan CloudFront distribusi Amazon dikonfigurasi untuk mengirimkan log akses ke bucket Amazon S3. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi tidak memiliki logging yang dikonfigurasi.
10.2.1.4	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	neptune-cluster-cloudwatch-log-ekspor diaktifkan	Pastikan klaster CloudWatch Amazon Neptunus mengaktifkan ekspor log untuk log audit. Aturannya adalah NON_COMPLIANT jika cluster Neptunus tidak mengaktifkan ekspor log untuk log audit. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.4	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	ecs-task-definition-log-konfigurasi	Pastikan bahwa LogConfiguration diatur pada Definisi Tugas ECS aktif. Aturan ini NON_COMPLIANT jika ECSTask Definisi aktif tidak memiliki sumber daya LogConfiguration yang ditentukan atau nilai untuk LogConfiguration adalah null dalam setidaknya satu definisi kontainer.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.4	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudtrail-diaktifkan	Catatan: Untuk aturan ini, pengidentifikasi aturan (CLOUD_TRAIL_ENABLED) dan nama aturan (cloudtrail-enabled) berbeda. Pastikan AWS CloudTrail jejak diaktifkan di AWS akun Anda. Aturannya adalah NON_COMPLIANT jika jejak tidak diaktifkan. Secara opsional, aturan memeriksa bucket S3 tertentu, topik Amazon Simple Notification Service (Amazon SNS), dan grup log. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.4	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	multi-region-cloudtrail-enabled	Catatan: untuk aturan ini, pengidentifikasi aturan (MULTI_REGION_CLOUD_TRAIL_ENABLED) dan nama aturan () berbeda. multi-region-cloudtrail-enabled Pastikan setidaknya ada satu multi-wilayah AWS CloudTrail. Aturannya adalah NON_COMPLIANT jika jejak tidak cocok dengan parameter input. Aturannya adalah NON_COMPLIANT jika ExcludeManagementEventSources bidang tidak kosong atau jika AWS CloudTrail dikonfigurasi untuk mengecualikan peristiwa manajemen seperti peristiwa AWS KMS atau peristiwa API Data Amazon RDS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.4	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	appsync-logging-enabled	Pastikan bahwa AWS AppSync API telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan, atau 'fieldLogLevel' bukan ERROR atau SEMUA.
10.2.1.4	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	waf-classic-logging-enabled	Pastikan pencatatan diaktifkan pada daftar kontrol akses web global klasik AWS WAF (web ACLs). Aturannya adalah NON_COMPLIANT untuk ACL web global, jika tidak mengaktifkan logging.
10.2.1.4	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-logging-diaktifkan	Pastikan pialang Amazon MQ mengaktifkan pencatatan CloudWatch audit Amazon. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.4	Log audit diimpleme ntasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-log-diaktifkan	Pastikan bahwa broker Amazon MQ mengaktif kan pencatatan CloudWatch audit. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.
10.2.1.4	Log audit diimpleme ntasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	eks-cluster-logging-enabled	Pastikan klaster Amazon Elastic Kubernetes Service (Amazon EKS) dikonfigurasi dengan logging diaktifkan. Aturannya adalah NON_COMPLIANT jika logging untuk klaster Amazon EKS tidak diaktifkan untuk semua jenis log.
10.2.1.4	Log audit diimpleme ntasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	elastic-beanstalk-logs-to-jam tangan awan	Pastikan lingkunga n AWS Elastic Beanstalk dikonfigu rasi untuk mengirim log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika nilai `StreamLogs` salah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.4	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	step-functions-state-machine-logging-diaktifkan	Pastikan bahwa mesin AWS Step Functions telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika mesin status tidak mengaktifkan logging atau konfigurasi logging tidak pada tingkat minimum yang disediakan.
10.2.1.4	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	netfw-logging-enabled	Pastikan firewall AWS Network Firewall telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika jenis logging tidak dikonfigurasi. Anda dapat menentukan jenis logging yang Anda ingin aturan untuk memeriksa.
10.2.1.5	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gwv2- access-logs-enabled	Pastikan bahwa tahap Amazon API Gateway V2 mengaktifkan pencatatan akses. Aturannya adalah NON_COMPLIANT jika 'accessLogSettings' tidak ada dalam konfigurasi Stage.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.5	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
10.2.1.5	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudfront-accesslogs-enabled	Pastikan CloudFront distribusi Amazon dikonfigurasi untuk mengirimkan log akses ke bucket Amazon S3. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi tidak memiliki logging yang dikonfigurasi.
10.2.1.5	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	neptune-cluster-cloudwatch-log-ekspor diaktifkan	Pastikan klaster CloudWatch Amazon Neptunus mengaktifkan ekspor log untuk log audit. Aturannya adalah NON_COMPLIANT jika cluster Neptunus tidak mengaktifkan ekspor log untuk log audit. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.5	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	ecs-task-definition-log-konfigurasi	Pastikan bahwa LogConfiguration diatur pada Definisi Tugas ECS aktif. Aturan ini NON_COMPLIANT jika ECSTask Definisi aktif tidak memiliki sumber daya LogConfiguration yang ditentukan atau nilai untuk LogConfiguration adalah null dalam setidaknya satu definisi kontainer.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.5	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudtrail-diaktifkan	Catatan: Untuk aturan ini, pengidentifikasi aturan (CLOUD_TRAIL_ENABLED) dan nama aturan (cloudtrail-enabled) berbeda. Pastikan AWS CloudTrail jejak diaktifkan di AWS akun Anda. Aturannya adalah NON_COMPLIANT jika jejak tidak diaktifkan. Secara opsional, aturan memeriksa bucket S3 tertentu, topik Amazon Simple Notification Service (Amazon SNS), dan grup log. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.5	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	multi-region-cloudtrail-enabled	Catatan: untuk aturan ini, pengidentifikasi aturan (MULTI_REGION_CLOUD_TRAIL_ENABLED) dan nama aturan () berbeda. multi-region-cloudtrail-enabled Pastikan setidaknya ada satu multi-wilayah AWS CloudTrail. Aturannya adalah NON_COMPLIANT jika jejak tidak cocok dengan parameter input. Aturannya adalah NON_COMPLIANT jika ExcludeManagementEventSources bidang tidak kosong atau jika AWS CloudTrail dikonfigurasi untuk mengecualikan peristiwa manajemen seperti peristiwa AWS KMS atau peristiwa API Data Amazon RDS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.5	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	appsync-logging-enabled	Pastikan bahwa AWS AppSync API telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan, atau 'fieldLogLevel' bukan ERROR atau SEMUA.
10.2.1.5	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	waf-classic-logging-enabled	Pastikan pencatatan diaktifkan pada daftar kontrol akses web global klasik AWS WAF (web ACLs). Aturannya adalah NON_COMPLIANT untuk ACL web global, jika tidak mengaktifkan logging.
10.2.1.5	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-logging-diaktifkan	Pastikan pialang Amazon MQ mengaktifkan pencatatan CloudWatch audit Amazon. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.5	Log audit diimpleme ntasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-log-diaktifkan	Pastikan bahwa broker Amazon MQ mengaktif kan pencatatan CloudWatch audit. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.
10.2.1.5	Log audit diimpleme ntasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	eks-cluster-logging-enabled	Pastikan klaster Amazon Elastic Kubernetes Service (Amazon EKS) dikonfigurasi dengan logging diaktifkan. Aturannya adalah NON_COMPLIANT jika logging untuk klaster Amazon EKS tidak diaktifkan untuk semua jenis log.
10.2.1.5	Log audit diimpleme ntasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	elastic-beanstalk-logs-to-jam tangan awan	Pastikan lingkunga n AWS Elastic Beanstalk dikonfigu rasi untuk mengirim log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika nilai `StreamLogs` salah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.5	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	step-functions-state-machine-logging-diaktifkan	Pastikan bahwa mesin AWS Step Functions telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika mesin status tidak mengaktifkan logging atau konfigurasi logging tidak pada tingkat minimum yang disediakan.
10.2.1.5	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	netfw-logging-enabled	Pastikan firewall AWS Network Firewall telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika jenis logging tidak dikonfigurasi. Anda dapat menentukan jenis logging yang Anda ingin aturan untuk memeriksa.
10.2.1.6	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gwv2- access-logs-enabled	Pastikan bahwa tahap Amazon API Gateway V2 mengaktifkan pencatatan akses. Aturannya adalah NON_COMPLIANT jika 'accessLogSettings' tidak ada dalam konfigurasi Stage.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.6	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
10.2.1.6	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudfront-accesslogs-enabled	Pastikan CloudFront distribusi Amazon dikonfigurasi untuk mengirimkan log akses ke bucket Amazon S3. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi tidak memiliki logging yang dikonfigurasi.
10.2.1.6	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	neptune-cluster-cloudwatch-log-ekspor diaktifkan	Pastikan klaster CloudWatch Amazon Neptunus mengaktifkan ekspor log untuk log audit. Aturannya adalah NON_COMPLIANT jika cluster Neptunus tidak mengaktifkan ekspor log untuk log audit. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.6	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	ecs-task-definition-log-konfigurasi	Pastikan bahwa LogConfiguration diatur pada Definisi Tugas ECS aktif. Aturan ini NON_COMPLIANT jika ECSTask Definisi aktif tidak memiliki sumber daya LogConfiguration yang ditentukan atau nilai untuk LogConfiguration adalah null dalam setidaknya satu definisi kontainer.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.6	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudtrail-diaktifkan	Catatan: Untuk aturan ini, pengidentifikasi aturan (CLOUD_TRAIL_ENABLED) dan nama aturan (cloudtrail-enabled) berbeda. Pastikan AWS CloudTrail jejak diaktifkan di AWS akun Anda. Aturannya adalah NON_COMPLIANT jika jejak tidak diaktifkan. Secara opsional, aturan memeriksa bucket S3 tertentu, topik Amazon Simple Notification Service (Amazon SNS), dan grup log. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.6	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	multi-region-cloudtrail-enabled	Catatan: untuk aturan ini, pengidentifikasi aturan (MULTI_REGION_CLOUD_TRAIL_ENABLED) dan nama aturan () berbeda. multi-region-cloudtrail-enabled Pastikan setidaknya ada satu multi-wilayah AWS CloudTrail. Aturannya adalah NON_COMPLIANT jika jejak tidak cocok dengan parameter input. Aturannya adalah NON_COMPLIANT jika ExcludeManagementEventSources bidang tidak kosong atau jika AWS CloudTrail dikonfigurasi untuk mengecualikan peristiwa manajemen seperti peristiwa AWS KMS atau peristiwa API Data Amazon RDS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.6	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	appsync-logging-enabled	Pastikan bahwa AWS AppSync API telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan, atau 'fieldLogLevel' bukan ERROR atau SEMUA.
10.2.1.6	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	waf-classic-logging-enabled	Pastikan pencatatan diaktifkan pada daftar kontrol akses web global klasik AWS WAF (web ACLs). Aturannya adalah NON_COMPLIANT untuk ACL web global, jika tidak mengaktifkan logging.
10.2.1.6	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-logging-diaktifkan	Pastikan pialang Amazon MQ mengaktifkan pencatatan CloudWatch audit Amazon. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.6	Log audit diimpleme ntasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-log-diaktifkan	Pastikan bahwa broker Amazon MQ mengaktif kan pencatatan CloudWatch audit. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.
10.2.1.6	Log audit diimpleme ntasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	eks-cluster-logging-enabled	Pastikan klaster Amazon Elastic Kubernetes Service (Amazon EKS) dikonfigurasi dengan logging diaktifkan. Aturannya adalah NON_COMPLIANT jika logging untuk klaster Amazon EKS tidak diaktifkan untuk semua jenis log.
10.2.1.6	Log audit diimpleme ntasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	elastic-beanstalk-logs-to-jam tangan awan	Pastikan lingkunga n AWS Elastic Beanstalk dikonfigu rasi untuk mengirim log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika nilai `StreamLogs` salah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.6	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	step-functions-state-machine-logging-diaktifkan	Pastikan bahwa mesin AWS Step Functions telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika mesin status tidak mengaktifkan logging atau konfigurasi logging tidak pada tingkat minimum yang disediakan.
10.2.1.6	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	netfw-logging-enabled	Pastikan firewall AWS Network Firewall telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika jenis logging tidak dikonfigurasi. Anda dapat menentukan jenis logging yang Anda ingin aturan untuk memeriksa.
10.2.1.7	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gwv2- access-logs-enabled	Pastikan bahwa tahap Amazon API Gateway V2 mengaktifkan pencatatan akses. Aturannya adalah NON_COMPLIANT jika 'accessLogSettings' tidak ada dalam konfigurasi Stage.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.7	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
10.2.1.7	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudfront-accesslogs-enabled	Pastikan CloudFront distribusi Amazon dikonfigurasi untuk mengirimkan log akses ke bucket Amazon S3. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi tidak memiliki logging yang dikonfigurasi.
10.2.1.7	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	neptune-cluster-cloudwatch-log-ekspor diaktifkan	Pastikan klaster CloudWatch Amazon Neptunus mengaktifkan ekspor log untuk log audit. Aturannya adalah NON_COMPLIANT jika cluster Neptunus tidak mengaktifkan ekspor log untuk log audit. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.7	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	ecs-task-definition-log-konfigurasi	Pastikan bahwa LogConfiguration diatur pada Definisi Tugas ECS aktif. Aturan ini NON_COMPLIANT jika ECSTask Definisi aktif tidak memiliki sumber daya LogConfiguration yang ditentukan atau nilai untuk LogConfiguration adalah null dalam setidaknya satu definisi kontainer.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.7	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudtrail-diaktifkan	Catatan: Untuk aturan ini, pengidentifikasi aturan (CLOUD_TRAIL_ENABLED) dan nama aturan (cloudtrail-enabled) berbeda. Pastikan AWS CloudTrail jejak diaktifkan di AWS akun Anda. Aturannya adalah NON_COMPLIANT jika jejak tidak diaktifkan. Secara opsional, aturan memeriksa bucket S3 tertentu, topik Amazon Simple Notification Service (Amazon SNS), dan grup log. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.7	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	multi-region-cloudtrail-enabled	Catatan: untuk aturan ini, pengidentifikasi aturan (MULTI_REGION_CLOUD_TRAIL_ENABLED) dan nama aturan () berbeda. multi-region-cloudtrail-enabled Pastikan setidaknya ada satu multi-wilayah AWS CloudTrail. Aturannya adalah NON_COMPLIANT jika jejak tidak cocok dengan parameter input. Aturannya adalah NON_COMPLIANT jika ExcludeManagementEventSources bidang tidak kosong atau jika AWS CloudTrail dikonfigurasi untuk mengecualikan peristiwa manajemen seperti peristiwa AWS KMS atau peristiwa API Data Amazon RDS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.7	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	appsync-logging-enabled	Pastikan bahwa AWS AppSync API telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan, atau 'fieldLogLevel' bukan ERROR atau SEMUA.
10.2.1.7	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	waf-classic-logging-enabled	Pastikan pencatatan diaktifkan pada daftar kontrol akses web global klasik AWS WAF (web ACLs). Aturannya adalah NON_COMPLIANT untuk ACL web global, jika tidak mengaktifkan logging.
10.2.1.7	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-logging-diaktifkan	Pastikan pialang Amazon MQ mengaktifkan pencatatan CloudWatch audit Amazon. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.7	Log audit diimpleme ntasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-log-diaktifkan	Pastikan bahwa broker Amazon MQ mengaktif kan pencatatan CloudWatch audit. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.
10.2.1.7	Log audit diimpleme ntasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	eks-cluster-logging-enabled	Pastikan klaster Amazon Elastic Kubernetes Service (Amazon EKS) dikonfigurasi dengan logging diaktifkan. Aturannya adalah NON_COMPLIANT jika logging untuk klaster Amazon EKS tidak diaktifkan untuk semua jenis log.
10.2.1.7	Log audit diimpleme ntasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	elastic-beanstalk-logs-to-jam tangan awan	Pastikan lingkunga n AWS Elastic Beanstalk dikonfigu rasi untuk mengirim log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika nilai `StreamLogs` salah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.1.7	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	step-functions-state-machine-logging-diaktifkan	Pastikan bahwa mesin AWS Step Functions telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika mesin status tidak mengaktifkan logging atau konfigurasi logging tidak pada tingkat minimum yang disediakan.
10.2.1.7	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	netfw-logging-enabled	Pastikan firewall AWS Network Firewall telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika jenis logging tidak dikonfigurasi. Anda dapat menentukan jenis logging yang Anda ingin aturan untuk memeriksa.
10.2.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gwv2- access-logs-enabled	Pastikan bahwa tahap Amazon API Gateway V2 mengaktifkan pencatatan akses. Aturannya adalah NON_COMPLIANT jika 'accessLogSettings' tidak ada dalam konfigurasi Stage.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
10.2.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudfront-accesslogs-enabled	Pastikan CloudFront distribusi Amazon dikonfigurasi untuk mengirimkan log akses ke bucket Amazon S3. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi tidak memiliki logging yang dikonfigurasi.
10.2.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	neptune-cluster-cloudwatch-log-ekspor diaktifkan	Pastikan klaster CloudWatch Amazon Neptunus mengaktifkan ekspor log untuk log audit. Aturannya adalah NON_COMPLIANT jika cluster Neptunus tidak mengaktifkan ekspor log untuk log audit. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	ecs-task-definition-log-konfigurasi	Pastikan bahwa LogConfiguration diatur pada Definisi Tugas ECS aktif. Aturan ini NON_COMPLIANT jika ECSTask Definisi aktif tidak memiliki sumber daya LogConfiguration yang ditentukan atau nilai untuk LogConfiguration adalah null dalam setidaknya satu definisi kontainer.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	cloudtrail-diaktifkan	Catatan: Untuk aturan ini, pengidentifikasi aturan (CLOUD_TRAIL_ENABLED) dan nama aturan (cloudtrail-enabled) berbeda. Pastikan AWS CloudTrail jejak diaktifkan di AWS akun Anda. Aturannya adalah NON_COMPLIANT jika jejak tidak diaktifkan. Secara opsional, aturan memeriksa bucket S3 tertentu, topik Amazon Simple Notification Service (Amazon SNS), dan grup log. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	multi-region-cloudtrail-enabled	Catatan: untuk aturan ini, pengidentifikasi aturan (MULTI_REGION_CLOUD_TRAIL_ENABLED) dan nama aturan () berbeda. multi-region-cloudtrail-enabled Pastikan setidaknya ada satu multi-wilayah AWS CloudTrail. Aturannya adalah NON_COMPLIANT jika jejak tidak cocok dengan parameter input. Aturannya adalah NON_COMPLIANT jika ExcludeManagementEventSources bidang tidak kosong atau jika AWS CloudTrail dikonfigurasi untuk mengecualikan peristiwa manajemen seperti peristiwa AWS KMS atau peristiwa API Data Amazon RDS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	appsync-logging-enabled	Pastikan bahwa AWS AppSync API telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan, atau 'fieldLogLevel' bukan ERROR atau SEMUA.
10.2.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	waf-classic-logging-enabled	Pastikan pencatatan diaktifkan pada daftar kontrol akses web global klasik AWS WAF (web ACLs). Aturannya adalah NON_COMPLIANT untuk ACL web global, jika tidak mengaktifkan logging.
10.2.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-logging-diaktifkan	Pastikan pialang Amazon MQ mengaktifkan pencatatan CloudWatch audit Amazon. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.2	Log audit diimpleme ntasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	mq-cloudwatch-audit-log-diaktifkan	Pastikan bahwa broker Amazon MQ mengaktif kan pencatatan CloudWatch audit. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.
10.2.2	Log audit diimpleme ntasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	eks-cluster-logging-enabled	Pastikan klaster Amazon Elastic Kubernetes Service (Amazon EKS) dikonfigurasi dengan logging diaktifkan. Aturannya adalah NON_COMPLIANT jika logging untuk klaster Amazon EKS tidak diaktifkan untuk semua jenis log.
10.2.2	Log audit diimpleme ntasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	elastic-beanstalk-logs-to-jam tangan awan	Pastikan lingkunga n AWS Elastic Beanstalk dikonfigu rasi untuk mengirim log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika nilai `StreamLogs` salah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.2.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	step-functions-state-machine-logging-diaktifkan	Pastikan bahwa mesin AWS Step Functions telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika mesin status tidak mengaktifkan logging atau konfigurasi logging tidak pada tingkat minimum yang disediakan.
10.2.2	Log audit diimplementasikan untuk mendukung deteksi anomali dan aktivitas mencurigakan, dan analisis forensik peristiwa. (PCI-DSS-V4.0)	netfw-logging-enabled	Pastikan firewall AWS Network Firewall telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika jenis logging tidak dikonfigurasi. Anda dapat menentukan jenis logging yang Anda ingin aturan untuk memeriksa.
10.3.1	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	api-gwv2- access-logs-enabled	Pastikan bahwa tahap Amazon API Gateway V2 mengaktifkan pencatatan akses. Aturannya adalah NON_COMPLIANT jika 'accessLogSettings' tidak ada dalam konfigurasi Stage.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.1	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
10.3.1	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	cloudfront-accesslogs-enabled	Pastikan CloudFront distribusi Amazon dikonfigurasi untuk mengirimkan log akses ke bucket Amazon S3. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi tidak memiliki logging yang dikonfigurasi.
10.3.1	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	neptune-cluster-cloudwatch-log-ekspor diaktifkan	Pastikan klaster CloudWatch Amazon Neptunus mengaktifkan ekspor log untuk log audit. Aturannya adalah NON_COMPLIANT jika cluster Neptunus tidak mengaktifkan ekspor log untuk log audit. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.1	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	ecs-task-definition-log-konfigurasi	Pastikan bahwa LogConfiguration diatur pada Definisi Tugas ECS aktif. Aturan ini NON_COMPL IANT jika ECSTask Definisi aktif tidak memiliki sumber daya LogConfiguration yang ditentukan atau nilai untuk LogConfig uration adalah null dalam setidaknya satu definisi kontainer.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.1	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	cloudtrail-diaktifkan	Catatan: Untuk aturan ini, pengidentifikasi aturan (CLOUD_TRAIL_ENABLED) dan nama aturan (cloudtrail-enabled) berbeda. Pastikan AWS CloudTrail jejak diaktifkan di AWS akun Anda. Aturannya adalah NON_COMPLIANT jika jejak tidak diaktifkan. Secara opsional, aturan memeriksa bucket S3 tertentu, topik Amazon Simple Notification Service (Amazon SNS), dan grup log. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.1	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	multi-region-cloudtrail-enabled	Catatan: untuk aturan ini, pengidentifikasi aturan (MULTI_REGION_CLOUD_TRAIL_ENABLED) dan nama aturan () berbeda. multi-region-cloudtrail-enabled Pastikan setidaknya ada satu multi-wilayah AWS CloudTrail. Aturannya adalah NON_COMPLIANT jika jejak tidak cocok dengan parameter input. Aturannya adalah NON_COMPLIANT jika ExcludeManagementEventSources bidang tidak kosong atau jika AWS CloudTrail dikonfigurasi untuk mengecualikan peristiwa manajemen seperti peristiwa AWS KMS atau peristiwa API Data Amazon RDS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.1	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	appsync-logging-enabled	Pastikan bahwa AWS AppSync API telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan, atau 'fieldLogLevel' bukan ERROR atau SEMUA.
10.3.1	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	waf-classic-logging-enabled	Pastikan pencatatan diaktifkan pada daftar kontrol akses web global klasik AWS WAF (web ACLs). Aturannya adalah NON_COMPLIANT untuk ACL web global, jika tidak mengaktifkan logging.
10.3.1	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	mq-cloudwatch-audit-logging-diaktifkan	Pastikan pialang Amazon MQ mengaktifkan pencatatan CloudWatch audit Amazon. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.1	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	mq-cloudwatch-audit-log-diaktifkan	Pastikan bahwa broker Amazon MQ mengaktif kan pencatatan CloudWatch audit. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.
10.3.1	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	eks-cluster-logging-enabled	Pastikan klaster Amazon Elastic Kubernetes Service (Amazon EKS) dikonfigurasi dengan logging diaktifkan. Aturannya adalah NON_COMPLIANT jika logging untuk klaster Amazon EKS tidak diaktifkan untuk semua jenis log.
10.3.1	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	elastic-beanstalk-logs-to-jam tangan awan	Pastikan lingkunga n AWS Elastic Beanstalk dikonfigu rasi untuk mengirim log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika nilai `StreamLogs` salah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.1	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	step-functions-state-machine-logging-diaktifkan	Pastikan bahwa mesin AWS Step Functions telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika mesin status tidak mengaktifkan logging atau konfigurasi logging tidak pada tingkat minimum yang disediakan.
10.3.1	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	netfw-logging-enabled	Pastikan firewall AWS Network Firewall telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika jenis logging tidak dikonfigurasi. Anda dapat menentukan jenis logging yang Anda ingin aturan untuk memeriksa.
10.3.2	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	cloudtrail-security-trail-enabled	Pastikan bahwa setidaknya ada satu AWS CloudTrail jejak yang ditentukan dengan praktik terbaik keamanan. Aturan ini SESUAI jika setidaknya ada satu jejak yang memenuhi semua hal berikut:

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.2	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	neptune-cluster-snapshot-public-dilarang	Pastikan snapshot kluster DB manual Amazon Neptunus tidak bersifat publik. Aturannya adalah NON_COMPLIANT jika ada snapshot cluster Neptunus yang ada dan yang baru bersifat publik.
10.3.2	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	docdb-cluster-snapshot-public-dilarang	Pastikan snapshot cluster manual Amazon DocumentDB tidak bersifat publik. Aturannya adalah NON_COMPLIANT jika ada snapshot cluster manual Amazon DocumentDB yang bersifat publik.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.2	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan brankas cadangan memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Aturannya adalah NON_COMPLIANT jika Brankas Cadangan tidak memiliki kebijakan berbasis sumber daya atau memiliki kebijakan tanpa pernyataan 'Deny' yang sesuai (pernyataan dengan cadangan: DeleteRecoveryPoint, cadangan:, dan cadangan: izin). UpdateRecoveryPointLifecycle PutBackupVaultAccessPolicy

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.2	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	emr-block-public-access	Pastikan akun dengan Amazon EMR telah mengaktif kan pengaturan akses publik yang memblokir. Aturannya adalah NON_COMPLIANT jika BlockPublicSecurityGroupRules salah, atau jika benar, port selain Port 22 terdaftar di. PermittedPublicSecurityGroupRuleRanges
10.3.2	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	s3- -blok access-point-public-access	Pastikan jalur akses Amazon S3 telah mengaktif kan pengaturan akses publik blokir. Aturannya adalah NON_COMPLIANT jika pengaturan akses publik blok tidak diaktifkan untuk titik akses S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.2	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	s3- -blok account-level-public-access	Pastikan bahwa pengaturan blok akses publik yang diperlukan dikonfigurasi dari tingkat akun. Aturannya hanya NON_COMPLIANT jika bidang yang ditetapkan di bawah ini tidak cocok dengan bidang yang sesuai di item konfigurasi.
10.3.2	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	s3- bucket-mfa-delete-enabled	Pastikan MFA Delete diaktifkan di konfigurasi pembuatan versi bucket Amazon Simple Storage Service (Amazon S3). Aturannya adalah NON_COMPLIANT jika MFA Delete tidak diaktifkan.
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	aurora-resources-protected-by-rencana cadangan	Pastikan klaster Amazon Aurora DB dilindungi oleh paket cadangan. Aturannya adalah NON_COMPLIANT jika Cluster Database Amazon Relational Database Service (Amazon RDS) tidak dilindungi oleh paket cadangan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	db-instance-backup-enabled	Pastikan instans RDS DB memiliki cadangan yang diaktifkan. Secara opsional, aturan memeriksa periode retensi cadangan dan jendela cadangan.
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	dynamodb-in-backup-plan	Pastikan tabel Amazon DynamoDB ada di AWS Paket Cadangan. Aturannya adalah NON_COMPLIANT jika tabel Amazon DynamoDB tidak ada dalam paket Backup apa pun. AWS
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	dynamodb-resources-protected-by-rencana cadangan	Pastikan tabel Amazon DynamoDB dilindungi oleh paket cadangan. Aturannya adalah NON_COMPLIANT jika Tabel DynamoDB tidak dicakup oleh rencana cadangan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	ebs-in-backup-plan	Pastikan volume Amazon Elastic Block Store (Amazon EBS) ditambahk an dalam paket cadangan Backup. AWS Aturannya adalah NON_COMPL IANT jika volume Amazon EBS tidak disertakan dalam paket cadangan.
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	ebs-resources-prot ected-by-rencana cadangan	Pastikan volume Amazon Elastic Block Store (Amazon EBS) dilindungi oleh paket cadangan. Aturannya adalah NON_COMPL IANT jika volume Amazon EBS tidak dicakup oleh paket cadangan.
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	ec2- -rencana resources-protected-by-backup	Pastikan instans Amazon Elastic Compute Cloud (Amazon EC2) dilindungi oleh paket cadangan. Aturannya adalah NON_COMPLIANT EC2 jika instance Amazon tidak dicakup oleh paket cadangan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	efs-in-backup-plan	Pastikan sistem file Amazon Elastic File System (Amazon EFS) ditambahk an dalam paket cadangan AWS Backup. Aturannya adalah NON_COMPL IANT jika sistem file EFS tidak disertaka n dalam paket cadangan.
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	efs-resources-prot ected-by-rencana cadangan	Pastikan sistem file Amazon Elastic File System (Amazon EFS) dilindungi oleh paket cadangan. Aturannya adalah NON_COMPLIANT jika Sistem File EFS tidak dicakup oleh rencana cadangan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	elasticache-redis-cluster-automatic-backup-periksa	Periksa apakah kluster Amazon ElastiCache Redis mengaktifkan cadangan otomatis. Aturannya adalah NON_COMPLIANT jika cluster SnapshotRetentionLimit for Redis kurang dari parameter . SnapshotRetentionPeriod Misalnya: Jika parameternya 15 maka aturannya tidak sesuai jika antara snapshotRetentionPeriod 0-15.
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	fsx-resources-protected-by-rencana cadangan	Pastikan Sistem FSx File Amazon dilindungi oleh paket cadangan. Aturannya adalah NON_COMPLIANT jika Sistem FSx File Amazon tidak dicakup oleh paket cadangan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	neptune-cluster-backup-retention-periksa	Pastikan periode retensi klaster Amazon Neptunus DB diatur ke jumlah hari tertentu. Aturannya adalah NON_COMPLIANT jika periode retensi kurang dari nilai yang ditentukan oleh parameter.
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	rds-in-backup-plan	Pastikan database Amazon Relational Database Service (Amazon RDS) hadir dalam AWS paket Backup. Aturannya adalah NON_COMPLIANT jika database Amazon RDS tidak disertakan dalam paket Backup apa pun. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	rds-resources-protected-by-rencana cadangan	Pastikan instans Amazon Relational Database Service (Amazon RDS) dilindungi oleh paket cadangan. Aturannya adalah NON_COMPLIANT jika instans Amazon RDS Database tidak dicakup oleh paket cadangan.
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	redshift-backup-enabled	Pastikan snapshot otomatis Amazon Redshift diaktifkan untuk cluster. Aturannya adalah NON_COMPLIANT jika nilai untuk automatedSnapshotRetention Periode lebih besar dari MaxRetentionPeriod atau kurang dari MinRetentionPeriod atau nilainya 0.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	s3- -rencana resources-protected-by-backup	Pastikan bucket Amazon Simple Storage Service (Amazon S3) dilindungi oleh paket cadangan. Aturannya adalah NON_COMPLIANT jika bucket Amazon S3 tidak tercakup oleh paket cadangan.
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	cloudtrail-security-trail-enabled	Pastikan bahwa setidaknya ada satu AWS CloudTrail jejak yang ditentukan dengan praktik terbaik keamanan. Aturan ini SESUAI jika setidaknya ada satu jejak yang memenuhi semua hal berikut:
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	db-instance-backup-enabled	Pastikan instans RDS DB memiliki cadangan yang diaktifkan. Secara opsional, aturan memeriksa periode retensi cadangan dan jendela cadangan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.3	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	dynamodb-pitr-enabled	Pastikan point-in-time pemulihan (PITR) diaktifkan untuk tabel Amazon DynamoDB. Aturannya adalah NON_COMPLIANT jika PITR tidak diaktifkan untuk tabel DynamoDB.
10.3.4	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	cloudfront-origin-access-identity-diaktifkan	Pastikan CloudFront distribusi dengan tipe Asal Amazon S3 memiliki identitas akses asal (OAI) yang dikonfigurasi. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi didukung oleh S3 dan jenis asal apa pun tidak dikonfigurasi OAI, atau asalnya bukan bucket S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.4	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	cloudfront-s3- origin-access-control-enabled	Pastikan CloudFront distribusi Amazon dengan tipe Asal Simple Storage Service (Amazon S3) Amazon S3 mengaktifkan kontrol akses asal (OAC). Aturannya adalah NON_COMPLIANT untuk CloudFront distribusi dengan asal Amazon S3 yang tidak mengaktifkan OAC.
10.3.4	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	s3- bucket-default-lock-enabled	Pastikan bucket S3 telah mengaktifkan kunci, secara default. Aturannya adalah NON_COMPLIANT jika kunci tidak diaktifkan.
10.3.4	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	s3- bucket-versioning-enabled	Pastikan pembuatan versi diaktifkan untuk bucket S3 Anda. Secara opsional, aturan memeriksa apakah penghapusan MFA diaktifkan untuk bucket S3 Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.3.4	Log audit dilindungi dari kehancuran dan modifikasi yang tidak sah. (PCI-DSS-V4.0)	cloudtrail-security-trail-enabled	Pastikan bahwa setidaknya ada satu AWS CloudTrail jejak yang ditentukan dengan praktik terbaik keamanan. Aturan ini SESUAI jika setidaknya ada satu jejak yang memenuhi semua hal berikut:
10.4.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
10.4.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	ec2- instance-detailed-monitoring-enabled	Pastikan pemantauan terperinci diaktifkan untuk EC2 instans. Aturannya adalah NON_COMPLIANT jika pemantauan terperinci tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	cloudwatch-alarm-resource-check	Pastikan bahwa jenis sumber daya memiliki CloudWatch alarm untuk metrik bernama. Untuk jenis sumber daya, Anda dapat menentukan volume EBS, EC2 instans, kluster Amazon RDS, atau bucket S3. Aturannya adalah COMPLIANT jika metrik bernama memiliki ID sumber daya dan CloudWatch alarm.
10.4.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	wafv2- rulegroup-logging-enabled	Pastikan pengumpulan metrik CloudWatch keamanan Amazon pada grup AWS WAFv2 aturan diaktifkan. Aturannya adalah NON_COMPLIANT jika '. VisibilityConfig CloudWatchMetricsEnabled'bidang disetel ke false.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	sns-topic-message-delivery-notifikasi-diaktifkan	Pastikan pencatatan Amazon Simple Notification Service (SNS) diaktifkan untuk status pengiriman pesan notifikasi yang dikirim ke topik untuk titik akhir. Aturannya adalah NON_COMPLIANT jika pemberitahuan status pengiriman untuk pesan tidak diaktifkan.
10.4.1.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
10.4.1.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	ec2- instance-detailed-monitoring-enabled	Pastikan pemantauan terperinci diaktifkan untuk EC2 instans. Aturannya adalah NON_COMPLIANT jika pemantauan terperinci tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.1.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.1.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.1.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.1.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	cloudwatch-alarm-resource-check	Pastikan bahwa jenis sumber daya memiliki CloudWatch alarm untuk metrik bernama. Untuk jenis sumber daya, Anda dapat menentukan volume EBS, EC2 instans, kluster Amazon RDS, atau bucket S3. Aturannya adalah COMPLIANT jika metrik bernama memiliki ID sumber daya dan CloudWatch alarm.
10.4.1.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	wafv2- rulegroup-logging-enabled	Pastikan pengumpulan metrik CloudWatch keamanan Amazon pada grup AWS WAFv2 aturan diaktifkan. Aturannya adalah NON_COMPLIANT jika '. VisibilityConfig CloudWatchMetricsEnabled'bidang disetel ke false.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.1.1	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	sns-topic-message-delivery-notifikasi-diaktifkan	Pastikan pencatatan Amazon Simple Notification Service (SNS) diaktifkan untuk status pengiriman pesan notifikasi yang dikirim ke topik untuk titik akhir. Aturannya adalah NON_COMPLIANT jika pemberitahuan status pengiriman untuk pesan tidak diaktifkan.
10.4.2	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
10.4.2	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	ec2- instance-detailed-monitoring-enabled	Pastikan pemantauan terperinci diaktifkan untuk EC2 instans. Aturannya adalah NON_COMPLIANT jika pemantauan terperinci tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.2	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.2	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.2	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.2	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	cloudwatch-alarm-resource-check	Pastikan bahwa jenis sumber daya memiliki CloudWatch alarm untuk metrik bernama. Untuk jenis sumber daya, Anda dapat menentukan volume EBS, EC2 instans, kluster Amazon RDS, atau bucket S3. Aturannya adalah COMPLIANT jika metrik bernama memiliki ID sumber daya dan CloudWatch alarm.
10.4.2	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	wafv2- rulegroup-logging-enabled	Pastikan pengumpulan metrik CloudWatch keamanan Amazon pada grup AWS WAFv2 aturan diaktifkan. Aturannya adalah NON_COMPLIANT jika '. VisibilityConfig CloudWatchMetricsEnabled'bidang disetel ke false.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.4.2	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	sns-topic-message-delivery-notifikasi-diaktifkan	Pastikan pencatatan Amazon Simple Notification Service (SNS) diaktifkan untuk status pengiriman pesan notifikasi yang dikirim ke topik untuk titik akhir. Aturannya adalah NON_COMPLIANT jika pemberitahuan status pengiriman untuk pesan tidak diaktifkan.
10.4.3	Log audit ditinjau untuk mengidentifikasi anomali atau aktivitas yang mencurigakan. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.5.1	Riwayat log audit dipertahankan dan tersedia untuk analisis. (PCI-DSS-V4.0)	cloudtrail-security-trail-enabled	Pastikan bahwa setidaknya ada satu AWS CloudTrail jejak yang ditentukan dengan praktik terbaik keamanan. Aturan ini SESUAI jika setidakny a ada satu jejak yang memenuhi semua hal berikut:
10.5.1	Riwayat log audit dipertahankan dan tersedia untuk analisis. (PCI-DSS-V4.0)	ec2- volume-inuse-check	Pastikan volume EBS dilampirkan ke EC2 instance. Secara opsional memastika n bahwa volume EBS ditandai untuk dihapus ketika sebuah instance dihentikan.
10.5.1	Riwayat log audit dipertahankan dan tersedia untuk analisis. (PCI-DSS-V4.0)	ecr-private-lifecycle-policy-dikonfigurasi	Pastikan bahwa repositori Amazon Elastic Container Registry (ECR) pribadi memiliki setidaknya satu kebijakan siklus hidup yang dikonfigu rasi. Aturannya adalah NON_COMPL IANT jika tidak ada kebijakan siklus hidup yang dikonfigu rasi untuk repositori pribadi ECR.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.5.1	Riwayat log audit dipertahankan dan tersedia untuk analisis. (PCI-DSS-V4.0)	dynamodb-pitr-enabled	Pastikan point-in-time pemulihan (PITR) diaktifkan untuk tabel Amazon DynamoDB. Aturannya adalah NON_COMPLIANT jika PITR tidak diaktifkan untuk tabel DynamoDB.
10.5.1	Riwayat log audit dipertahankan dan tersedia untuk analisis. (PCI-DSS-V4.0)	cw-loggroup-retention-period-periksa	Pastikan periode CloudWatch LogGroup retensi Amazon diatur ke lebih dari 365 hari atau periode retensi tertentu. Aturannya adalah NON_COMPLIANT jika periode retensi kurang dari MinRetentionTime, jika ditentukan, atau 365 hari.
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	api-gwv2- access-logs-enabled	Pastikan bahwa tahap Amazon API Gateway V2 mengaktifkan pencatatan akses. Aturannya adalah NON_COMPLIANT jika 'accessLogSettings' tidak ada dalam konfigurasi Stage.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	cloudfront-accesslogs-enabled	Pastikan CloudFront distribusi Amazon dikonfigurasi untuk mengirimkan log akses ke bucket Amazon S3. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi tidak memiliki logging yang dikonfigurasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	s3- bucket-blacklisted-actions-prohibited	Pastikan kebijakan bucket Amazon Simple Storage Service (Amazon S3) tidak mengizinkan tindakan tingkat ember dan tingkat objek yang diblokir pada sumber daya dalam bucket untuk prinsipal dari akun lain. AWS Misalnya, aturan memeriksa bahwa kebijakan bucket Amazon S3 tidak mengizinkan AWS akun lain untuk melakukan tindakan s3: GetBucket * dan s3: DeleteObject pada objek apa pun di bucket. Aturannya adalah NON_COMPLIANT jika ada tindakan yang diblokir yang diizinkan oleh kebijakan bucket Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	s3- bucket-policy-not-more -permisif	Pastikan kebijakan bucket Amazon Simple Storage Service (S3) Anda tidak mengizinkan izin antar akun selain kebijakan bucket Amazon S3 kontrol yang Anda berikan.
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	neptune-cluster-cloudwatch-log-ekspor diaktifkan	Pastikan klaster CloudWatch Amazon Neptunus mengaktifkan ekspor log untuk log audit. Aturannya adalah NON_COMPLIANT jika cluster Neptunus tidak mengaktifkan ekspor log untuk log audit. CloudWatch
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	ec2- instance-detailed-monitoring-enabled	Pastikan pemantauan terperinci diaktifkan untuk EC2 instans. Aturannya adalah NON_COMPLIANT jika pemantauan terperinci tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	ecs-task-definition-log-konfigurasi	Pastikan bahwa LogConfiguration diatur pada Definisi Tugas ECS aktif. Aturan ini NON_COMPLIANT jika ECSTask Definisi aktif tidak memiliki sumber daya LogConfiguration yang ditentukan atau nilai untuk LogConfiguration adalah null dalam setidaknya satu definisi kontainer.
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	cloudwatch-alarm-resource-check	Pastikan bahwa jenis sumber daya memiliki CloudWatch alarm untuk metrik bernama. Untuk jenis sumber daya, Anda dapat menentukan volume EBS, EC2 instans, kluster Amazon RDS, atau bucket S3. Aturannya adalah COMPLIANT jika metrik bernama memiliki ID sumber daya dan CloudWatch alarm.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	cloudtrail-diaktifkan	Catatan: Untuk aturan ini, pengidentifikasi aturan (CLOUD_TRAIL_ENABLED) dan nama aturan (cloudtrail-enabled) berbeda. Pastikan AWS CloudTrail jejak diaktifkan di AWS akun Anda. Aturannya adalah NON_COMPLIANT jika jejak tidak diaktifkan. Secara opsional, aturan memeriksa bucket S3 tertentu, topik Amazon Simple Notification Service (Amazon SNS), dan grup log. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	multi-region-cloudtrail-enabled	Catatan: untuk aturan ini, pengidentifikasi aturan (MULTI_REGION_CLOUD_TRAIL_ENABLED) dan nama aturan () berbeda. multi-region-cloudtrail-enabled Pastikan setidaknya ada satu multi-wilayah AWS CloudTrail. Aturannya adalah NON_COMPLIANT jika jejak tidak cocok dengan parameter input. Aturannya adalah NON_COMPLIANT jika ExcludeManagementEventSources bidang tidak kosong atau jika AWS CloudTrail dikonfigurasi untuk mengecualikan peristiwa manajemen seperti peristiwa AWS KMS atau peristiwa API Data Amazon RDS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	appsync-logging-enabled	Pastikan bahwa AWS AppSync API telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan, atau 'fieldLogLevel' bukan ERROR atau SEMUA.
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	waf-classic-logging-enabled	Pastikan pencatatan diaktifkan pada daftar kontrol akses web global klasik AWS WAF (web ACLs). Aturannya adalah NON_COMPLIANT untuk ACL web global, jika tidak mengaktifkan logging.
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	mq-cloudwatch-audit-logging-diaktifkan	Pastikan pialang Amazon MQ mengaktifkan pencatatan CloudWatch audit Amazon. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	mq-cloudwatch-audit-log-diaktifkan	Pastikan bahwa broker Amazon MQ mengaktifkan pencatatan CloudWatch audit. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	eks-cluster-logging-enabled	Pastikan klaster Amazon Elastic Kubernetes Service (Amazon EKS) dikonfigurasi dengan logging diaktifkan. Aturannya adalah NON_COMPLIANT jika logging untuk klaster Amazon EKS tidak diaktifkan untuk semua jenis log.
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	elastic-beanstalk-logs-to-jam tangan awan	Pastikan lingkungan AWS Elastic Beanstalk dikonfigurasi untuk mengirim log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika nilai `StreamLogs` salah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	wafv2- rulegroup-logging-enabled	Pastikan pengumpulan metrik CloudWatch keamanan Amazon pada grup AWS WAFv2 aturan diaktifkan. Aturannya adalah NON_COMPLIANT jika '. VisibilityConfig CloudWatchMetricsEnabled'bidang disetel ke false.
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	sns-topic-message-delivery-notifikasi-diaktifkan	Pastikan pencatatan Amazon Simple Notification Service (SNS) diaktifkan untuk status pengiriman pesan notifikasi yang dikirim ke topik untuk titik akhir. Aturannya adalah NON_COMPLIANT jika pemberitahuan status pengiriman untuk pesan tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	step-functions-state-machine-logging-diaktifkan	Pastikan bahwa mesin AWS Step Functions telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika mesin status tidak mengaktifkan logging atau konfigurasi logging tidak pada tingkat minimum yang disediakan.
10.6.3	Mekanisme sinkronisasi waktu mendukung pengaturan waktu yang konsisten di semua sistem. (PCI-DSS-V4.0)	netfw-logging-enabled	Pastikan firewall AWS Network Firewall telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika jenis logging tidak dikonfigurasi. Anda dapat menentukan jenis logging yang Anda ingin aturan untuk memeriksa.
10.7.1	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.7.1	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	cloudformation-stack-notification-check	Pastikan CloudFormation tumpukan Anda mengirim pemberitahuan acara ke topik Amazon SNS. Secara opsional pastikan bahwa topik Amazon SNS yang ditentukan digunakan. Aturannya adalah NON_COMPLIANT jika CloudFormation tumpukan tidak mengirim notifikasi.
10.7.1	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	ec2- instance-detailed-monitoring-enabled	Pastikan pemantauan terperinci diaktifkan untuk EC2 instans. Aturannya adalah NON_COMPLIANT jika pemantauan terperinci tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.7.1	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.7.1	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.7.1	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.7.1	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	cloudwatch-alarm-resource-check	Pastikan bahwa jenis sumber daya memiliki CloudWatch alarm untuk metrik bernama. Untuk jenis sumber daya, Anda dapat menentukan volume EBS, EC2 instans, kluster Amazon RDS, atau bucket S3. Aturannya adalah COMPLIANT jika metrik bernama memiliki ID sumber daya dan CloudWatch alarm.
10.7.1	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	wafv2- rulegroup-logging-enabled	Pastikan pengumpulan metrik CloudWatch keamanan Amazon pada grup AWS WAFv2 aturan diaktifkan. Aturannya adalah NON_COMPLIANT jika '. VisibilityConfig CloudWatchMetricsEnabled'bidang disetel ke false.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.7.1	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	sns-topic-message-delivery-notifikasi-diaktifkan	Pastikan pencatatan Amazon Simple Notification Service (SNS) diaktifkan untuk status pengiriman pesan notifikasi yang dikirim ke topik untuk titik akhir. Aturannya adalah NON_COMPLIANT jika pemberitahuan status pengiriman untuk pesan tidak diaktifkan.
10.7.2	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.7.2	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	cloudformation-stack-notification-check	Pastikan CloudFormation tumpukan Anda mengirim pemberitahuan acara ke topik Amazon SNS. Secara opsional pastikan bahwa topik Amazon SNS yang ditentukan digunakan. Aturannya adalah NON_COMPLIANT jika CloudFormation tumpukan tidak mengirim notifikasi.
10.7.2	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	ec2- instance-detailed-monitoring-enabled	Pastikan pemantauan terperinci diaktifkan untuk EC2 instans. Aturannya adalah NON_COMPLIANT jika pemantauan terperinci tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.7.2	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.7.2	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.7.2	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.7.2	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	cloudwatch-alarm-resource-check	Pastikan bahwa jenis sumber daya memiliki CloudWatch alarm untuk metrik bernama. Untuk jenis sumber daya, Anda dapat menentukan volume EBS, EC2 instans, kluster Amazon RDS, atau bucket S3. Aturannya adalah COMPLIANT jika metrik bernama memiliki ID sumber daya dan CloudWatch alarm.
10.7.2	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	wafv2- rulegroup-logging-enabled	Pastikan pengumpulan metrik CloudWatch keamanan Amazon pada grup AWS WAFv2 aturan diaktifkan. Aturannya adalah NON_COMPLIANT jika '. VisibilityConfig CloudWatchMetricsEnabled'bidang disetel ke false.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
10.7.2	Kegagalan sistem kontrol keamanan kritis terdeteksi, dilaporkan, dan ditanggapi dengan segera. (PCI-DSS-V4.0)	sns-topic-message-delivery-notifikasi-diaktifkan	Pastikan pencatatan Amazon Simple Notification Service (SNS) diaktifkan untuk status pengiriman pesan notifikasi yang dikirim ke topik untuk titik akhir. Aturannya adalah NON_COMPLIANT jika pemberitahuan status pengiriman untuk pesan tidak diaktifkan.
11.5.2	Intrusi jaringan dan perubahan file yang tidak terduga terdeteksi dan ditanggapi. (PCI-DSS-V4.0)	cloudformation-stack-notification-check	Pastikan CloudFormation tumpukan Anda mengirim pemberitahuan acara ke topik Amazon SNS. Secara opsional pastikan bahwa topik Amazon SNS yang ditentukan digunakan. Aturannya adalah NON_COMPLIANT jika CloudFormation tumpukan tidak mengirim notifikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.5.2	Intrusi jaringan dan perubahan file yang tidak terduga terdeteksi dan ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.5.2	Intrusi jaringan dan perubahan file yang tidak terduga terdeteksi dan ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.
11.5.2	Intrusi jaringan dan perubahan file yang tidak terduga terdeteksi dan ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-settings-check	Pastikan CloudWatch alarm dengan nama metrik yang diberikan memiliki pengaturan yang ditentukan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.5.2	Intrusi jaringan dan perubahan file yang tidak terduga terdeteksi dan ditanggapi. (PCI-DSS-V4.0)	sns-topic-message-delivery-notifikasi-diaktifkan	Pastikan pencatatan Amazon Simple Notification Service (SNS) diaktifkan untuk status pengiriman pesan notifikasi yang dikirim ke topik untuk titik akhir. Aturannya adalah NON_COMPLIANT jika pemberitahuan status pengiriman untuk pesan tidak diaktifkan.
11.6.1	Perubahan yang tidak sah pada halaman pembayaran terdeteksi dan ditanggapi. (PCI-DSS-V4.0)	cloudformation-stack-notification-check	Pastikan CloudFormation tumpukan Anda mengirim pemberitahuan acara ke topik Amazon SNS. Secara opsional pastikan bahwa topik Amazon SNS yang ditentukan digunakan. Aturannya adalah NON_COMPLIANT jika CloudFormation tumpukan tidak mengirim notifikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.6.1	Perubahan yang tidak sah pada halaman pembayaran terdeteksi dan ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.6.1	Perubahan yang tidak sah pada halaman pembayaran terdeteksi dan ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.
11.6.1	Perubahan yang tidak sah pada halaman pembayaran terdeteksi dan ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-settings-check	Pastikan CloudWatch alarm dengan nama metrik yang diberikan memiliki pengaturan yang ditentukan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
11.6.1	Perubahan yang tidak sah pada halaman pembayaran terdeteksi dan ditanggapi. (PCI-DSS-V4.0)	sns-topic-message-delivery-notifikasi-diaktifkan	Pastikan pencatatan Amazon Simple Notification Service (SNS) diaktifkan untuk status pengiriman pesan notifikasi yang dikirim ke topik untuk titik akhir. Aturannya adalah NON_COMPLIANT jika pemberitahuan status pengiriman untuk pesan tidak diaktifkan.
12.10.5	Insiden keamanan yang dicurigai dan dikonfirmasi yang dapat berdampak pada CDE segera ditanggapi. (PCI-DSS-V4.0)	cloudformation-stack-notification-check	Pastikan CloudFormation tumpukan Anda mengirim pemberitahuan acara ke topik Amazon SNS. Secara opsional pastikan bahwa topik Amazon SNS yang ditentukan digunakan. Aturannya adalah NON_COMPLIANT jika CloudFormation tumpukan tidak mengirim notifikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.10.5	Insiden keamanan yang dicurigai dan dikonfirmasi yang dapat berdampak pada CDE segera ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.10.5	Insiden keamanan yang dicurigai dan dikonfirmasi yang dapat berdampak pada CDE segera ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.
12.10.5	Insiden keamanan yang dicurigai dan dikonfirmasi yang dapat berdampak pada CDE segera ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-settings-check	Pastikan CloudWatch alarm dengan nama metrik yang diberikan memiliki pengaturan yang ditentukan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
12.10.5	Insiden keamanan yang dicurigai dan dikonfirmasi yang dapat berdampak pada CDE segera ditanggapi. (PCI-DSS-V4.0)	sns-topic-message-delivery-notifikasi-diaktifkan	Pastikan pencatatan Amazon Simple Notification Service (SNS) diaktifkan untuk status pengiriman pesan notifikasi yang dikirim ke topik untuk titik akhir. Aturannya adalah NON_COMPLIANT jika pemberitahuan status pengiriman untuk pesan tidak diaktifkan.
12.4.2.1	Kepatuhan PCI DSS dikelola. (PCI-DSS-V4.0)	service-catalog-shared-within-organisasi	Pastikan bahwa AWS Service Catalog membagikan portofolio ke organisasi (kumpulan AWS akun yang diperlakukan sebagai satu unit) saat integrasi diaktifkan dengan Organizations AWS . Aturannya adalah NON_COMPLIANT jika nilai `Type` dari sebuah share adalah `ACCOUNT`.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.5	Komponen sistem dikonfigurasi dan dikelola dengan aman. (PCI-DSS-V4.0)	cloudfront-security-policy-check	Pastikan CloudFront distribusi Amazon menggunakan kebijakan keamanan minimum dan rangkaian sandi TLSv1 0,2 atau lebih tinggi untuk koneksi penampil. Aturan ini adalah NON_COMPLIANT untuk CloudFront distribusi jika di bawah .2_2018 minimumProtocolVersion . TLSv1
2.2.5	Komponen sistem dikonfigurasi dan dikelola dengan aman. (PCI-DSS-V4.0)	cloudfront-sni-enabled	Pastikan CloudFront distribusi Amazon menggunakan sertifikat SSL khusus dan dikonfigurasi untuk menggunakan SNI untuk melayani permintaan HTTPS. Aturannya adalah NON_COMPLIANT jika sertifikat SSL khusus dikaitkan tetapi metode dukungan SSL adalah alamat IP khusus.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.5	Komponen sistem dikonfigurasi dan dikelola dengan aman. (PCI-DSS-V4.0)	transfer-family-server-no-ftp	Pastikan server yang dibuat dengan AWS Transfer Family tidak menggunakan FTP untuk koneksi endpoint. Aturannya adalah NON_COMPLIANT jika protokol server untuk koneksi endpoint diaktifkan FTP.
2.2.5	Komponen sistem dikonfigurasi dan dikelola dengan aman. (PCI-DSS-V4.0)	cloudfront-no-deprecated-ssl-protokol	Pastikan CloudFront distribusi tidak menggunakan protokol SSL yang tidak digunakan lagi untuk komunikasi HTTPS antara lokasi tepi dan asal kustom. CloudFront Aturan ini adalah NON_COMPLIANT untuk CloudFront distribusi jika ada 'termasuk'. OriginSslProtocols SSLv3

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.5	Komponen sistem dikonfigurasi dan dikelola dengan aman. (PCI-DSS-V4.0)	cloudfront-traffic-to-origin-dienkripsi	Pastikan CloudFront distribusi Amazon mengenkripsi lalu lintas ke asal kustom. Aturannya adalah NON_COMPLIANT jika '' is'http-only' atau jika' 'adalah OriginProtocolPolicy 'match-viewer' dan' 'allow-all'. OriginProtocolPolicy ViewerProtocolPolicy
2.2.5	Komponen sistem dikonfigurasi dan dikelola dengan aman. (PCI-DSS-V4.0)	cloudfront-viewer-policy-https	Pastikan CloudFront distribusi Amazon Anda menggunakan HTTPS (secara langsung atau melalui pengalihan). Aturannya adalah NON_COMPLIANT jika nilai ViewerProtocolPolicy disetel ke 'allow-all' untuk atau untuk. DefaultCacheBehavior CacheBehaviors

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.7	Komponen sistem dikonfigurasi dan dikelola dengan aman. (PCI-DSS-V4.0)	dms-redis-tls-enabled	Pastikan titik akhir AWS Database Migration Service (AWS DMS) untuk penyimpanan data Redis diaktifkan untuk TLS/SSL encryption of data communicated with other endpoints. The rule is NON_COMPLIANT if TLS/SSL enkripsi tidak diaktifkan.
2.2.7	Komponen sistem dikonfigurasi dan dikelola dengan aman. (PCI-DSS-V4.0)	cloudfront-no-deprecated-ssl-protokol	Pastikan CloudFront distribusi tidak menggunakan protokol SSL yang tidak digunakan lagi untuk komunikasi HTTPS antara lokasi tepi dan asal kustom. CloudFront Aturan ini adalah NON_COMPLIANT untuk CloudFront distribusi jika ada 'termasuk'. OriginSslProtocols SSLv3

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.7	Komponen sistem dikonfigurasi dan dikelola dengan aman. (PCI-DSS-V4.0)	cloudfront-traffic-to-origin-dienkripsi	Pastikan CloudFront distribusi Amazon mengenkripsi lalu lintas ke asal kustom. Aturannya adalah NON_COMPLIANT jika '' is'http-only' atau jika' 'adalah OriginProtocolPolicy 'match-viewer' dan' 'allow-all'. OriginProtocolPolicy ViewerProtocolPolicy
2.2.7	Komponen sistem dikonfigurasi dan dikelola dengan aman. (PCI-DSS-V4.0)	cloudfront-viewer-policy-https	Pastikan CloudFront distribusi Amazon Anda menggunakan HTTPS (secara langsung atau melalui pengalihan). Aturannya adalah NON_COMPLIANT jika nilai ViewerProtocolPolicy disetel ke 'allow-all' untuk atau untuk. DefaultCacheBehavior CacheBehaviors

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.7	Komponen sistem dikonfigurasi dan dikelola dengan aman. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.
2.2.7	Komponen sistem dikonfigurasi dan dikelola dengan aman. (PCI-DSS-V4.0)	dax-tls-endpoint-encryption	Pastikan klaster Amazon DynamoDB Accelerator (DAX) Anda telah disetel ke TLS. ClusterEndpointEncryptionType Aturannya adalah NON_COMPLIANT jika cluster DAX tidak dienkripsi oleh transport layer security (TLS).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
2.2.7	Komponen sistem dikonfigurasi dan dikelola dengan aman. (PCI-DSS-V4.0)	msk-in-cluster-node-membutuhkan-tls	Pastikan bahwa klaster MSK Amazon memberlakukan enkripsi dalam perjalanan menggunakan HTTPS (TLS) dengan node broker klaster. Aturannya adalah NON_COMPLIANT jika komunikasi teks biasa diaktifkan untuk koneksi node broker in-cluster.
2.2.7	Komponen sistem dikonfigurasi dan dikelola dengan aman. (PCI-DSS-V4.0)	dms-endpoint-ssl-configured	Pastikan titik akhir AWS Database Migration Service (AWS DMS) dikonfigurasi dengan koneksi SSL. Aturannya adalah NON_COMPLIANT jika AWS DMS tidak memiliki koneksi SSL yang dikonfigurasi.
3.2.1	Penyimpanan data akun dijaga seminimal mungkin. (PCI-DSS-V4.0)	ec2- volume-inuse-check	Pastikan volume EBS dilampirkan ke EC2 instance. Secara opsional memastikan bahwa volume EBS ditandai untuk dihapus ketika sebuah instance dihentikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.2.1	Penyimpanan data akun dijaga seminimal mungkin. (PCI-DSS-V4.0)	ecr-private-lifecycle-policy-dikonfigurasi	Pastikan bahwa repositori Amazon Elastic Container Registry (ECR) pribadi memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi. Aturannya adalah NON_COMPLIANT jika tidak ada kebijakan siklus hidup yang dikonfigurasi untuk repositori pribadi ECR.
3.2.1	Penyimpanan data akun dijaga seminimal mungkin. (PCI-DSS-V4.0)	dynamodb-pitr-enabled	Pastikan point-in-time pemulihan (PITR) diaktifkan untuk tabel Amazon DynamoDB. Aturannya adalah NON_COMPLIANT jika PITR tidak diaktifkan untuk tabel DynamoDB.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.2.1	Penyimpanan data akun dijaga seminimal mungkin. (PCI-DSS-V4.0)	cw-loggroup-retention-period-periksa	Pastikan periode CloudWatch LogGroup retensi Amazon diatur ke lebih dari 365 hari atau periode retensi tertentu. Aturannya adalah NON_COMPLIANT jika periode retensi kurang dari MinRetentionTime, jika ditentukan, atau 365 hari.
3.3.1.1	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	ec2- volume-inuse-check	Pastikan volume EBS dilampirkan ke EC2 instance. Secara opsional memastikan bahwa volume EBS ditandai untuk dihapus ketika sebuah instance dihentikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1.1	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	ecr-private-lifecycle-policy-dikonfigurasi	Pastikan bahwa repositori Amazon Elastic Container Registry (ECR) pribadi memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi. Aturannya adalah NON_COMPLIANT jika tidak ada kebijakan siklus hidup yang dikonfigurasi untuk repositori pribadi ECR.
3.3.1.1	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	dynamodb-pitr-enabled	Pastikan point-in-time pemulihan (PITR) diaktifkan untuk tabel Amazon DynamoDB. Aturannya adalah NON_COMPLIANT jika PITR tidak diaktifkan untuk tabel DynamoDB.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1.1	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	cw-loggroup-retention-period-periksa	Pastikan periode CloudWatch LogGroup retensi Amazon diatur ke lebih dari 365 hari atau periode retensi tertentu. Aturannya adalah NON_COMPLIANT jika periode retensi kurang dari MinRetentionTime, jika ditentukan, atau 365 hari.
3.3.1.3	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	ec2- volume-inuse-check	Pastikan volume EBS dilampirkan ke EC2 instance. Secara opsional memastikan bahwa volume EBS ditandai untuk dihapus ketika sebuah instance dihentikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1.3	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	ecr-private-lifecycle-policy-dikonfigurasi	Pastikan bahwa repositori Amazon Elastic Container Registry (ECR) pribadi memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi. Aturannya adalah NON_COMPLIANT jika tidak ada kebijakan siklus hidup yang dikonfigurasi untuk repositori pribadi ECR.
3.3.1.3	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	dynamodb-pitr-enabled	Pastikan point-in-time pemulihan (PITR) diaktifkan untuk tabel Amazon DynamoDB. Aturannya adalah NON_COMPLIANT jika PITR tidak diaktifkan untuk tabel DynamoDB.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.1.3	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	cw-loggroup-retention-period-periksa	Pastikan periode CloudWatch LogGroup retensi Amazon diatur ke lebih dari 365 hari atau periode retensi tertentu. Aturannya adalah NON_COMPLIANT jika periode retensi kurang dari MinRetentionTime, jika ditentukan, atau 365 hari.
3.3.2	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	ec2- volume-inuse-check	Pastikan volume EBS dilampirkan ke EC2 instance. Secara opsional memastikan bahwa volume EBS ditandai untuk dihapus ketika sebuah instance dihentikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.2	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	ecr-private-lifecycle-policy-dikonfigurasi	Pastikan bahwa repositori Amazon Elastic Container Registry (ECR) pribadi memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi. Aturannya adalah NON_COMPLIANT jika tidak ada kebijakan siklus hidup yang dikonfigurasi untuk repositori pribadi ECR.
3.3.2	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	dynamodb-pitr-enabled	Pastikan point-in-time pemulihan (PITR) diaktifkan untuk tabel Amazon DynamoDB. Aturannya adalah NON_COMPLIANT jika PITR tidak diaktifkan untuk tabel DynamoDB.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.2	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	cw-loggroup-retention-period-periksa	Pastikan periode CloudWatch LogGroup retensi Amazon diatur ke lebih dari 365 hari atau periode retensi tertentu. Aturannya adalah NON_COMPLIANT jika periode retensi kurang dari MinRetentionTime, jika ditentukan, atau 365 hari.
3.3.3	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	ec2- volume-inuse-check	Pastikan volume EBS dilampirkan ke EC2 instance. Secara opsional memastikan bahwa volume EBS ditandai untuk dihapus ketika sebuah instance dihentikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.3	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	ecr-private-lifecycle-policy-dikonfigurasi	Pastikan bahwa repositori Amazon Elastic Container Registry (ECR) pribadi memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi. Aturannya adalah NON_COMPLIANT jika tidak ada kebijakan siklus hidup yang dikonfigurasi untuk repositori pribadi ECR.
3.3.3	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	dynamodb-pitr-enabled	Pastikan point-in-time pemulihan (PITR) diaktifkan untuk tabel Amazon DynamoDB. Aturannya adalah NON_COMPLIANT jika PITR tidak diaktifkan untuk tabel DynamoDB.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3.3	Data otentikasi sensitif (SAD) tidak disimpan setelah otorisasi. (PCI-DSS-V4.0)	cw-loggroup-retention-period-periksa	Pastikan periode CloudWatch LogGroup retensi Amazon diatur ke lebih dari 365 hari atau periode retensi tertentu. Aturannya adalah NON_COMPLIANT jika periode retensi kurang dari MinRetentionTime, jika ditentukan, atau 365 hari.
3.5.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	athena-workgroup-encrypted-at-istirahat	Pastikan bahwa workgroup Amazon Athena dienkripsi saat istirahat. Aturannya adalah NON_COMPLIANT jika enkripsi data saat istirahat tidak diaktifkan untuk workgroup Athena.
3.5.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	neptune-cluster-snapshot-encrypted	Pastikan bahwa kluster Amazon Neptunus DB memiliki snapshot yang dienkripsi. Aturannya adalah NON_COMPLIANT jika cluster Neptunus tidak memiliki snapshot yang dienkripsi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	redshift-cluster-kms-enabled	Pastikan klaster Amazon Redshift menggunakan AWS kunci Key Management Service (AWS KMS) yang ditentukan untuk enkripsi. Aturannya adalah COMPLIANT jika enkripsi diaktifkan dan cluster dienkrips i dengan kunci yang disediakan dalam parameter. kmsKeyArn Aturannya adalah NON_COMPL IANT jika cluster tidak dienkripsi atau dienkripsi dengan kunci lain.
3.5.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	codebuild-project-artifact-encryption	Pastikan bahwa sebuah AWS CodeBuild proyek telah mengaktifkan enkripsi untuk semua artefaknya. Aturannya adalah NON_COMPL IANT jika 'Encrypti onDisabled' disetel ke 'true' untuk konfigura si artefak primer atau sekunder (jika ada).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	codebuild-project-s3-log-terenkripsi	Pastikan AWS CodeBuild proyek yang dikonfigurasi dengan Amazon S3 Logs mengaktif kan enkripsi untuk lognya. Aturannya adalah NON_COMPL IANT jika 'Encrypti onDisabled' disetel ke 'true' di S3 proyek. LogsConfig CodeBuild
3.5.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	dax-encryption-ena bled	Pastikan klaster Amazon DynamoDB Accelerator (DAX) dienkripsi. Aturannya adalah NON_COMPL IANT jika cluster DAX tidak dienkripsi.
3.5.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	eks-secrets-encrypted	Pastikan bahwa klaster Amazon Elastic Kubernete s Service dikonfigu rasi agar rahasia Kubernetes dienkrips i menggunakan kunci Key Management Service (KMS). AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	api-gw-cache-enabled-dan-dienkripsi	Pastikan bahwa semua metode dalam tahapan Amazon API Gateway telah mengaktifkan cache dan cache dienkripsi. Aturannya adalah NON_COMPLIANT jika metode apa pun dalam tahap Amazon API Gateway tidak dikonfigurasi ke cache atau cache tidak dienkripsi.
3.5.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	docdb-cluster-encrypted	Pastikan enkripsi penyimpanan diaktifkan untuk klaster Amazon DocumentDB Anda (dengan kompatibilitas MongoDB). Aturannya adalah NON_COMPLIANT jika enkripsi penyimpanan tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	dynamodb-table-encrypted-kms	Pastikan tabel Amazon DynamoDB dienkripsi AWS dengan Key Management Service (KMS). Aturannya adalah NON_COMPLIANT jika tabel Amazon DynamoDB tidak dienkripsi dengan KMS. AWS Aturannya juga NON_COMPLIANT jika kunci AWS KMS terenkripsi tidak ada dalam parameter input. kmsKeyArns
3.5.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	dynamodb-table-encryption-enabled	Pastikan tabel Amazon DynamoDB dienkripsi dan memeriksa statusnya . Aturannya SESUAI jika status diaktifkan atau diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	codebuild-project-envvar-awscred-periksa	Pastikan bahwa proyek TIDAK berisi variabel lingkungan AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY. Aturannya adalah NON_COMPLIANT ketika variabel lingkungan proyek berisi kredenal teks biasa.
3.5.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	eks-cluster-secrets-encrypted	Pastikan bahwa klaster Amazon EKS tidak dikonfigurasi agar rahasia Kubernetes dienkripsi menggunakan KMS. AWS Aturannya adalah NON_COMPLIANT jika kluster EKS tidak memiliki sumber daya EncryptionConfig atau jika EncryptionConfig tidak menyebutkan rahasia sebagai sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	kinesis-stream-encrypted	Pastikan aliran Amazon Kinesis dienkripsi saat istirahat dengan enkripsi sisi server. Aturannya adalah NON_COMPLIANT untuk aliran Kinesis jika " StreamEncryption tidak ada.
3.5.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	neptune-cluster-encrypted	Pastikan enkripsi penyimpanan diaktifkan untuk kluster Amazon Neptunus DB Anda. Aturannya adalah NON_COMPLIANT jika enkripsi penyimpanan tidak diaktifkan.
3.5.1.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	acm-pca-root-ca-dinonaktifkan	Pastikan AWS Private Certificate Authority (AWS Private CA) memiliki CA root yang dinonaktifkan. Aturannya adalah NON_COMPLIANT untuk root CAs dengan status yang tidak DINONAKTIFKAN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.1.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	cloudfront-custom-ssl-certificate	Pastikan sertifikat yang terkait dengan CloudFront distribusi Amazon bukan sertifikat SSL default. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi menggunakan sertifikat SSL default.
3.5.1.1	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.1.3	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	acm-pca-root-ca-di nonaktifkan	Pastikan AWS Private Certificate Authority (AWS Private CA) memiliki CA root yang dinonaktifkan. Aturannya adalah NON_COMPLIANT untuk root CAs dengan status yang tidak DINONAKTI FKAN.
3.5.1.3	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	cloudfront-custom-ssl-certificate	Pastikan sertifikat yang terkait dengan CloudFront distribus i Amazon bukan sertifikat SSL default. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi menggunak an sertifikat SSL default.
3.5.1.3	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	neptune-cluster-sn apshot-public-dilarang	Pastikan snapshot kluster DB manual Amazon Neptunus tidak bersifat publik. Aturannya adalah NON_COMPLIANT jika ada snapshot cluster Neptunus yang ada dan yang baru bersifat publik.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.1.3	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	docdb-cluster-snapshot-public-dilarang	Pastikan snapshot cluster manual Amazon DocumentDB tidak bersifat publik. Aturannya adalah NON_COMPLIANT jika ada snapshot cluster manual Amazon DocumentDB yang bersifat publik.
3.5.1.3	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan brankas cadangan memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Aturannya adalah NON_COMPLIANT jika Brankas Cadangan tidak memiliki kebijakan berbasis sumber daya atau memiliki kebijakan tanpa pernyataan 'Deny' yang sesuai (pernyataan dengan cadangan: DeleteRecoveryPoint, cadangan:, dan cadangan: izin). UpdateRecoveryPointLifecycle PutBackupVaultAccessPolicy

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.1.3	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.1.3	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	emr-block-public-access	Pastikan akun dengan Amazon EMR telah mengaktif kan pengaturan akses publik yang memblokir. Aturannya adalah NON_COMPL IANT jika BlockPubl icSecurityGroupRules salah, atau jika benar, port selain Port 22 terdaftar di. Permitted PublicSecurityGrou pRuleRanges
3.5.1.3	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	s3- -blok access-point-public-access	Pastikan jalur akses Amazon S3 telah mengaktif kan pengaturan akses publik blokir. Aturannya adalah NON_COMPLIANT jika pengaturan akses publik blok tidak diaktifkan untuk titik akses S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5.1.3	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	s3- -blok account-level-public-access	Pastikan bahwa pengaturan blok akses publik yang diperlukan dikonfigurasi dari tingkat akun. Aturannya hanya NON_COMPLIANT jika bidang yang ditetapkan di bawah ini tidak cocok dengan bidang yang sesuai di item konfigurasi.
3.5.1.3	Nomor akun utama (PAN) diamankan di mana pun disimpan. (PCI-DSS-V4.0)	s3- bucket-mfa-delete-enabled	Pastikan MFA Delete diaktifkan di konfigurasi pembuatan versi bucket Amazon Simple Storage Service (Amazon S3). Aturannya adalah NON_COMPLIANT jika MFA Delete tidak diaktifkan.
3.6.1	Kunci kriptografi yang digunakan untuk melindungi data akun yang disimpan diamankan. (PCI-DSS-V4.0)	acm-pca-root-ca-dinonaktifkan	Pastikan AWS Private Certificate Authority (AWS Private CA) memiliki CA root yang dinonaktifkan. Aturannya adalah NON_COMPLIANT untuk root CAs dengan status yang tidak DINONAKTIFKAN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.1	Kunci kriptografi yang digunakan untuk melindungi data akun yang disimpan diamankan. (PCI-DSS-V4.0)	cloudfront-custom-ssl-certificate	Pastikan sertifikat yang terkait dengan CloudFront distribusi Amazon bukan sertifikat SSL default. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi menggunakan sertifikat SSL default.
3.6.1	Kunci kriptografi yang digunakan untuk melindungi data akun yang disimpan diamankan. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.1.2	Kunci kriptografi yang digunakan untuk melindungi data akun yang disimpan diamankan. (PCI-DSS-V4.0)	acm-pca-root-ca-dinonaktifkan	Pastikan AWS Private Certificate Authority (AWS Private CA) memiliki CA root yang dinonaktifkan. Aturannya adalah NON_COMPLIANT untuk root CAs dengan status yang tidak DINONAKTIFKAN.
3.6.1.2	Kunci kriptografi yang digunakan untuk melindungi data akun yang disimpan diamankan. (PCI-DSS-V4.0)	cloudfront-custom-ssl-certificate	Pastikan sertifikat yang terkait dengan CloudFront distribusi Amazon bukan sertifikat SSL default. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi menggunakan sertifikat SSL default.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.1.2	Kunci kriptografi yang digunakan untuk melindungi data akun yang disimpan diamankan. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.
3.6.1.3	Kunci kriptografi yang digunakan untuk melindungi data akun yang disimpan diamankan. (PCI-DSS-V4.0)	acm-pca-root-ca-dinonaktifkan	Pastikan AWS Private Certificate Authority (AWS Private CA) memiliki CA root yang dinonaktifkan. Aturannya adalah NON_COMPLIANT untuk root CAs dengan status yang tidak DINONAKTIFKAN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.1.3	Kunci kriptografi yang digunakan untuk melindungi data akun yang disimpan diamankan. (PCI-DSS-V4.0)	cloudfront-custom-ssl-certificate	Pastikan sertifikat yang terkait dengan CloudFront distribusi Amazon bukan sertifikat SSL default. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi menggunakan sertifikat SSL default.
3.6.1.3	Kunci kriptografi yang digunakan untuk melindungi data akun yang disimpan diamankan. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.1.4	Kunci kriptografi yang digunakan untuk melindungi data akun yang disimpan diamankan. (PCI-DSS-V4.0)	acm-pca-root-ca-dinonaktifkan	Pastikan AWS Private Certificate Authority (AWS Private CA) memiliki CA root yang dinonaktifkan. Aturannya adalah NON_COMPLIANT untuk root CAs dengan status yang tidak DINONAKTIFKAN.
3.6.1.4	Kunci kriptografi yang digunakan untuk melindungi data akun yang disimpan diamankan. (PCI-DSS-V4.0)	cloudfront-custom-ssl-certificate	Pastikan sertifikat yang terkait dengan CloudFront distribusi Amazon bukan sertifikat SSL default. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi menggunakan sertifikat SSL default.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.6.1.4	Kunci kriptografi yang digunakan untuk melindungi data akun yang disimpan diamankan. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.
3.7.1	Di mana kriptografi digunakan untuk melindungi data akun yang tersimpan, proses dan prosedur manajemen kunci yang mencakup semua aspek siklus hidup utama didefinisikan dan diimplementasikan. (PCI-DSS-V4.0)	acm-certificate-rsa-check	Pastikan sertifikat RSA yang dikelola oleh AWS Certificate Manager (ACM) memiliki panjang kunci minimal '2048' bit. Aturannya adalah NON_COMPLIANT jika panjang kunci minimum kurang dari 2048 bit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.7.1	Di mana kriptografi digunakan untuk melindungi data akun yang tersimpan, proses dan prosedur manajemen kunci yang mencakup semua aspek siklus hidup utama didefinisikan dan diimplementasikan. (PCI-DSS-V4.0)	acm-pca-root-ca-dinonaktifkan	Pastikan AWS Private Certificate Authority (AWS Private CA) memiliki CA root yang dinonaktifkan. Aturannya adalah NON_COMPLIANT untuk root CAs dengan status yang tidak DINONAKTIFKAN.
3.7.1	Di mana kriptografi digunakan untuk melindungi data akun yang tersimpan, proses dan prosedur manajemen kunci yang mencakup semua aspek siklus hidup utama didefinisikan dan diimplementasikan. (PCI-DSS-V4.0)	cloudfront-custom-ssl-certificate	Pastikan sertifikat yang terkait dengan CloudFront distribusi Amazon bukan sertifikat SSL default. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi menggunakan sertifikat SSL default.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.7.1	Di mana kriptografi digunakan untuk melindungi data akun yang tersimpan, proses dan prosedur manajemen kunci yang mencakup semua aspek siklus hidup utama didefinisikan dan diimplementasikan. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.
3.7.2	Di mana kriptografi digunakan untuk melindungi data akun yang tersimpan, proses dan prosedur manajemen kunci yang mencakup semua aspek siklus hidup utama didefinisikan dan diimplementasikan. (PCI-DSS-V4.0)	acm-pca-root-ca-dinonaktifkan	Pastikan AWS Private Certificate Authority (AWS Private CA) memiliki CA root yang dinonaktifkan. Aturannya adalah NON_COMPLIANT untuk root CAs dengan status yang tidak DINONAKTIFKAN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.7.2	Di mana kriptogra fi digunakan untuk melindungi data akun yang tersimpan, proses dan prosedur manajemen kunci yang mencakup semua aspek siklus hidup utama didefinis ikan dan diimpleme ntasikan. (PCI-DSS-V4.0)	cloudfront-custom-ssl-certificate	Pastikan sertifikat yang terkait dengan CloudFront distribus i Amazon bukan sertifikat SSL default. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi menggunak an sertifikat SSL default.
3.7.2	Di mana kriptogra fi digunakan untuk melindungi data akun yang tersimpan, proses dan prosedur manajemen kunci yang mencakup semua aspek siklus hidup utama didefinis ikan dan diimpleme ntasikan. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunak an sertifikat SSL yang disediaka n oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Applicati on Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.7.4	Di mana kriptografi digunakan untuk melindungi data akun yang tersimpan, proses dan prosedur manajemen kunci yang mencakup semua aspek siklus hidup utama didefinisikan dan diimplementasikan. (PCI-DSS-V4.0)	acm-pca-root-ca-dinonaktifkan	Pastikan AWS Private Certificate Authority (AWS Private CA) memiliki CA root yang dinonaktifkan. Aturannya adalah NON_COMPLIANT untuk root CAs dengan status yang tidak DINONAKTIFKAN.
3.7.4	Di mana kriptografi digunakan untuk melindungi data akun yang tersimpan, proses dan prosedur manajemen kunci yang mencakup semua aspek siklus hidup utama didefinisikan dan diimplementasikan. (PCI-DSS-V4.0)	cloudfront-custom-ssl-certificate	Pastikan sertifikat yang terkait dengan CloudFront distribusi Amazon bukan sertifikat SSL default. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi menggunakan sertifikat SSL default.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.7.4	Di mana kriptografi digunakan untuk melindungi data akun yang tersimpan, proses dan prosedur manajemen kunci yang mencakup semua aspek siklus hidup utama didefinisikan dan diimplementasikan. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.
3.7.6	Di mana kriptografi digunakan untuk melindungi data akun yang tersimpan, proses dan prosedur manajemen kunci yang mencakup semua aspek siklus hidup utama didefinisikan dan diimplementasikan. (PCI-DSS-V4.0)	acm-pca-root-ca-dinonaktifkan	Pastikan AWS Private Certificate Authority (AWS Private CA) memiliki CA root yang dinonaktifkan. Aturannya adalah NON_COMPLIANT untuk root CAs dengan status yang tidak DINONAKTIFKAN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.7.6	Di mana kriptografi digunakan untuk melindungi data akun yang tersimpan, proses dan prosedur manajemen kunci yang mencakup semua aspek siklus hidup utama didefinisikan dan diimplementasikan. (PCI-DSS-V4.0)	cloudfront-custom-ssl-certificate	Pastikan sertifikat yang terkait dengan CloudFront distribusi Amazon bukan sertifikat SSL default. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi menggunakan sertifikat SSL default.
3.7.6	Di mana kriptografi digunakan untuk melindungi data akun yang tersimpan, proses dan prosedur manajemen kunci yang mencakup semua aspek siklus hidup utama didefinisikan dan diimplementasikan. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.7.7	Di mana kriptografi digunakan untuk melindungi data akun yang tersimpan, proses dan prosedur manajemen kunci yang mencakup semua aspek siklus hidup utama didefinisikan dan diimplementasikan. (PCI-DSS-V4.0)	acm-pca-root-ca-dinonaktifkan	Pastikan AWS Private Certificate Authority (AWS Private CA) memiliki CA root yang dinonaktifkan. Aturannya adalah NON_COMPLIANT untuk root CAs dengan status yang tidak DINONAKTIFKAN.
3.7.7	Di mana kriptografi digunakan untuk melindungi data akun yang tersimpan, proses dan prosedur manajemen kunci yang mencakup semua aspek siklus hidup utama didefinisikan dan diimplementasikan. (PCI-DSS-V4.0)	cloudfront-custom-ssl-certificate	Pastikan sertifikat yang terkait dengan CloudFront distribusi Amazon bukan sertifikat SSL default. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi menggunakan sertifikat SSL default.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.7.7	Di mana kriptografi digunakan untuk melindungi data akun yang tersimpan, proses dan prosedur manajemen kunci yang mencakup semua aspek siklus hidup utama didefinisikan dan diimplementasikan. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancer. Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.2.1	PAN dilindungi dengan kriptografi yang kuat selama transmisi. (PCI-DSS-V4.0)	dms-redis-tls-enabled	Pastikan titik akhir AWS Database Migration Service (AWS DMS) untuk penyimpanan data Redis diaktifkan untuk TLS/SSL encryption of data communicated with other endpoints. The rule is NON_COMPLIANT if TLS/SSL enkripsi tidak diaktifkan.
4.2.1	PAN dilindungi dengan kriptografi yang kuat selama transmisi. (PCI-DSS-V4.0)	cloudfront-no-deprecated-ssl-protokol	Pastikan CloudFront distribusi tidak menggunakan protokol SSL yang tidak digunakan lagi untuk komunikasi HTTPS antara lokasi tepi dan asal kustom. CloudFront Aturan ini adalah NON_COMPLIANT untuk CloudFront distribusi jika ada 'termasuk'. OriginSslProtocols SSLv3

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.2.1	PAN dilindungi dengan kriptografi yang kuat selama transmisi. (PCI-DSS-V4.0)	cloudfront-traffic-to-origin-dienkripsi	Pastikan CloudFront distribusi Amazon mengenkripsi lalu lintas ke asal kustom. Aturannya adalah NON_COMPLIANT jika '' is'http-only' atau jika' 'adalah OriginProtocolPolicy 'match-viewer' dan' 'allow-all'. OriginProtocolPolicy ViewerProtocolPolicy
4.2.1	PAN dilindungi dengan kriptografi yang kuat selama transmisi. (PCI-DSS-V4.0)	cloudfront-viewer-policy-https	Pastikan CloudFront distribusi Amazon Anda menggunakan HTTPS (secara langsung atau melalui pengalihan). Aturannya adalah NON_COMPLIANT jika nilai ViewerProtocolPolicy disetel ke 'allow-all' untuk atau untuk. DefaultCacheBehavior CacheBehaviors

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.2.1	PAN dilindungi dengan kriptografi yang kuat selama transmisi. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancers . Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.
4.2.1	PAN dilindungi dengan kriptografi yang kuat selama transmisi. (PCI-DSS-V4.0)	dax-tls-endpoint-encryption	Pastikan klaster Amazon DynamoDB Accelerator (DAX) Anda telah disetel ke TLS. ClusterEndpointEncryptionType Aturannya adalah NON_COMPLIANT jika cluster DAX tidak dienkripsi oleh transport layer security (TLS).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.2.1	PAN dilindungi dengan kriptografi yang kuat selama transmisi. (PCI-DSS-V4.0)	msk-in-cluster-node-membutuhkan-tls	Pastikan bahwa klaster MSK Amazon memberlakukan enkripsi dalam perjalanan menggunakan HTTPS (TLS) dengan node broker klaster. Aturannya adalah NON_COMPLIANT jika komunikasi teks biasa diaktifkan untuk koneksi node broker in-cluster.
4.2.1	PAN dilindungi dengan kriptografi yang kuat selama transmisi. (PCI-DSS-V4.0)	dms-endpoint-ssl-configured	Pastikan titik akhir AWS Database Migration Service (AWS DMS) dikonfigurasi dengan koneksi SSL. Aturannya adalah NON_COMPLIANT jika AWS DMS tidak memiliki koneksi SSL yang dikonfigurasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.2.1.1	PAN dilindungi dengan kriptografi yang kuat selama transmisi. (PCI-DSS-V4.0)	acm-pca-root-ca-dinonaktifkan	Pastikan AWS Private Certificate Authority (AWS Private CA) memiliki CA root yang dinonaktifkan. Aturannya adalah NON_COMPLIANT untuk root CAs dengan status yang tidak DINONAKTIFKAN.
4.2.1.1	PAN dilindungi dengan kriptografi yang kuat selama transmisi. (PCI-DSS-V4.0)	cloudfront-custom-ssl-certificate	Pastikan sertifikat yang terkait dengan CloudFront distribusi Amazon bukan sertifikat SSL default. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi menggunakan sertifikat SSL default.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.2.1.1	PAN dilindungi dengan kriptografi yang kuat selama transmisi. (PCI-DSS-V4.0)	dms-redis-tls-enabled	Pastikan titik akhir AWS Database Migration Service (AWS DMS) untuk penyimpanan data Redis diaktifkan untuk TLS/SSL encryption of data communicated with other endpoints. The rule is NON_COMPLIANT if TLS/SSL enkripsi tidak diaktifkan.
4.2.1.1	PAN dilindungi dengan kriptografi yang kuat selama transmisi. (PCI-DSS-V4.0)	cloudfront-no-deprecated-ssl-protokol	Pastikan CloudFront distribusi tidak menggunakan protokol SSL yang tidak digunakan lagi untuk komunikasi HTTPS antara lokasi tepi dan asal kustom. CloudFront Aturan ini adalah NON_COMPLIANT untuk CloudFront distribusi jika ada 'termasuk'. OriginSslProtocols SSLv3

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.2.1.1	PAN dilindungi dengan kriptografi yang kuat selama transmisi. (PCI-DSS-V4.0)	cloudfront-traffic-to-origin-dienkripsi	Pastikan CloudFront distribusi Amazon mengenkripsi lalu lintas ke asal kustom. Aturannya adalah NON_COMPLIANT jika '' is'http-only' atau jika' 'adalah OriginProtocolPolicy 'match-viewer' dan' 'allow-all'. OriginProtocolPolicy ViewerProtocolPolicy
4.2.1.1	PAN dilindungi dengan kriptografi yang kuat selama transmisi. (PCI-DSS-V4.0)	cloudfront-viewer-policy-https	Pastikan CloudFront distribusi Amazon Anda menggunakan HTTPS (secara langsung atau melalui pengalihan). Aturannya adalah NON_COMPLIANT jika nilai ViewerProtocolPolicy disetel ke 'allow-all' untuk atau untuk. DefaultCacheBehavior CacheBehaviors

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.2.1.1	PAN dilindungi dengan kriptografi yang kuat selama transmisi. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancers . Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.
4.2.1.1	PAN dilindungi dengan kriptografi yang kuat selama transmisi. (PCI-DSS-V4.0)	dax-tls-endpoint-encryption	Pastikan klaster Amazon DynamoDB Accelerator (DAX) Anda telah disetel ke TLS. ClusterEndpointEncryptionType Aturannya adalah NON_COMPLIANT jika cluster DAX tidak dienkripsi oleh transport layer security (TLS).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.2.1.1	PAN dilindungi dengan kriptografi yang kuat selama transmisi. (PCI-DSS-V4.0)	msk-in-cluster-node-membutuhkan-tls	Pastikan bahwa klaster MSK Amazon memberlakukan enkripsi dalam perjalanan menggunakan HTTPS (TLS) dengan node broker klaster. Aturannya adalah NON_COMPLIANT jika komunikasi teks biasa diaktifkan untuk koneksi node broker in-cluster.
4.2.1.1	PAN dilindungi dengan kriptografi yang kuat selama transmisi. (PCI-DSS-V4.0)	dms-endpoint-ssl-configured	Pastikan titik akhir AWS Database Migration Service (AWS DMS) dikonfigurasi dengan koneksi SSL. Aturannya adalah NON_COMPLIANT jika AWS DMS tidak memiliki koneksi SSL yang dikonfigurasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	api-gwv2- access-logs-enabled	Pastikan bahwa tahap Amazon API Gateway V2 mengaktifkan pencatatan akses. Aturannya adalah NON_COMPLIANT jika 'accessLogSettings' tidak ada dalam konfigurasi Stage.
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	cloudfront-accesslogs-enabled	Pastikan CloudFront distribusi Amazon dikonfigurasi untuk mengirimkan log akses ke bucket Amazon S3. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi tidak memiliki logging yang dikonfigurasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	cloudtrail-security-trail-enabled	Pastikan bahwa setidaknya ada satu AWS CloudTrail jejak yang ditentukan dengan praktik terbaik keamanan. Aturan ini SESUAI jika setidakny a ada satu jejak yang memenuhi semua hal berikut:
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	neptune-cluster-cl oudwatch-log-ekspor diaktifkan	Pastikan klaster CloudWatch Amazon Neptunus mengaktif kan ekspor log untuk log audit. Aturannya adalah NON_COMPL IANT jika cluster Neptunus tidak mengaktifkan ekspor log untuk log audit. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	ecs-task-definition-log-konfigurasi	Pastikan bahwa LogConfiguration diatur pada Definisi Tugas ECS aktif. Aturan ini NON_COMPL IANT jika ECSTask Definisi aktif tidak memiliki sumber daya LogConfiguration yang ditentukan atau nilai untuk LogConfig uration adalah null dalam setidaknya satu definisi kontainer.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	cloudtrail-diaktifkan	Catatan: Untuk aturan ini, pengidentifikasi aturan (CLOUD_TRAIL_ENABLED) dan nama aturan (cloudtrail-enabled) berbeda. Pastikan AWS CloudTrail jejak diaktifkan di AWS akun Anda. Aturannya adalah NON_COMPLIANT jika jejak tidak diaktifkan. Secara opsional, aturan memeriksa bucket S3 tertentu, topik Amazon Simple Notification Service (Amazon SNS), dan grup log. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	multi-region-cloudtrail-enabled	Catatan: untuk aturan ini, pengidentifikasi aturan (MULTI_REGION_CLOUD_TRAIL_ENABLED) dan nama aturan () berbeda. multi-region-cloudtrail-enabled Pastikan setidaknya ada satu multi-wilayah AWS CloudTrail. Aturannya adalah NON_COMPLIANT jika jejak tidak cocok dengan parameter input. Aturannya adalah NON_COMPLIANT jika ExcludeManagementEventSources bidang tidak kosong atau jika AWS CloudTrail dikonfigurasi untuk mengecualikan peristiwa manajemen seperti peristiwa AWS KMS atau peristiwa API Data Amazon RDS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	appsync-logging-enabled	Pastikan bahwa AWS AppSync API telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan, atau 'fieldLogLevel' bukan ERROR atau SEMUA.
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	waf-classic-logging-enabled	Pastikan pencatatan diaktifkan pada daftar kontrol akses web global klasik AWS WAF (web ACLs). Aturannya adalah NON_COMPLIANT untuk ACL web global, jika tidak mengaktifkan logging.
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	mq-cloudwatch-audit-logging-diaktifkan	Pastikan pialang Amazon MQ mengaktifkan pencatatan CloudWatch audit Amazon. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	mq-cloudwatch-audit-log-diaktifkan	Pastikan bahwa broker Amazon MQ mengaktif kan pencatatan CloudWatch audit. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	eks-cluster-logging-enabled	Pastikan klaster Amazon Elastic Kubernetes Service (Amazon EKS) dikonfigurasi dengan logging diaktifkan. Aturannya adalah NON_COMPLIANT jika logging untuk klaster Amazon EKS tidak diaktifkan untuk semua jenis log.
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	elastic-beanstalk-logs-to-jam tangan awan	Pastikan lingkunga n AWS Elastic Beanstalk dikonfigu rasi untuk mengirim log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika nilai `StreamLogs` salah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	step-functions-state-machine-logging-diaktifkan	Pastikan bahwa mesin AWS Step Functions telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika mesin status tidak mengaktifkan logging atau konfigurasi logging tidak pada tingkat minimum yang disediakan.
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	netfw-logging-enabled	Pastikan firewall AWS Network Firewall telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika jenis logging tidak dikonfigurasi. Anda dapat menentukan jenis logging yang Anda ingin aturan untuk memeriksa.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
5.3.4	Mekanisme dan proses anti-malware aktif, dipelihara, dan dipantau. (PCI-DSS-V4.0)	cw-loggroup-retention-period-periksa	Pastikan periode CloudWatch LogGroup retensi Amazon diatur ke lebih dari 365 hari atau periode retensi tertentu. Aturannya adalah NON_COMPLIANT jika periode retensi kurang dari MinRetentionTime, jika ditentukan, atau 365 hari.
6.3.3	Kerentanan keamanan diidentifikasi dan ditangani. (PCI-DSS-V4.0)	lambda-function-settings-check	Pastikan setelan fungsi AWS Lambda untuk runtime, role, timeout, dan ukuran memori sesuai dengan nilai yang diharapkan. Aturan mengabaikan fungsi dengan tipe paket 'Gambar' dan fungsi dengan runtime disetel ke 'OS-Only Runtime'. Aturannya adalah NON_COMPLIANT jika pengaturan fungsi Lambda tidak cocok dengan nilai yang diharapkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.3.3	Kerentanan keamanan diidentif ikasi dan ditangani. (PCI-DSS-V4.0)	eks-cluster-oldest-supported-versi	Pastikan klaster Amazon Elastic Kubernetes Service (EKS) tidak menjalank an versi tertua yang didukung. Aturannya adalah NON_COMPL IANT jika kluster EKS menjalankan versi tertua yang didukung (sama dengan parameter "oldestVersionSup ported).
6.4.1	Aplikasi web yang menghadap publik dilindungi dari serangan. (PCI-DSS-V4.0)	cloudfront-associated-with-waf	Pastikan CloudFron t distribusi Amazon dikaitkan dengan firewall aplikasi web (WAF) atau daftar kontrol akses WAFv2 web (ACLs). Aturannya adalah NON_COMPLIANT jika CloudFront distribusi tidak terkait dengan ACL web WAF.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.4.1	Aplikasi web yang menghadap publik dilindungi dari serangan. (PCI-DSS-V4.0)	appsync-associated-with-waf	Pastikan AWS AppSync APIs yang terkait dengan daftar kontrol akses AWS WAFv2 web (ACLs). Aturannya adalah NON_COMPLIANT untuk AWS AppSync API jika tidak terkait dengan ACL web.
6.4.1	Aplikasi web yang menghadap publik dilindungi dari serangan. (PCI-DSS-V4.0)	wafv2- webacl-not-empty	Pastikan bahwa ACL WAFv2 Web berisi aturan WAF atau grup aturan WAF. Aturan ini NON_COMPL IANT jika ACL Web tidak berisi aturan WAF atau grup aturan WAF.
6.4.1	Aplikasi web yang menghadap publik dilindungi dari serangan. (PCI-DSS-V4.0)	wafv2- rulegroup-not-empty	Pastikan bahwa Grup WAFv2 Aturan berisi aturan. Aturannya adalah NON_COMPL IANT jika tidak ada aturan dalam Grup Aturan. WAFv2

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.4.1	Aplikasi web yang menghadap publik dilindungi dari serangan. (PCI-DSS-V4.0)	waf-global-webacl-not-kosong	Pastikan bahwa WAF Global Web ACL berisi beberapa aturan WAF atau grup aturan. Aturan ini adalah NON_COMPLIANT jika ACL Web tidak berisi aturan WAF atau grup aturan.
6.4.1	Aplikasi web yang menghadap publik dilindungi dari serangan. (PCI-DSS-V4.0)	waf-global-rulegroup-not-kosong	Pastikan grup aturan AWS WAF Classic berisi beberapa aturan. Aturannya adalah NON_COMPLIANT jika tidak ada aturan yang ada dalam grup aturan.
6.4.1	Aplikasi web yang menghadap publik dilindungi dari serangan. (PCI-DSS-V4.0)	waf-global-rulegroup-not-kosong	Pastikan grup aturan AWS WAF Classic berisi beberapa aturan. Aturannya adalah NON_COMPLIANT jika tidak ada aturan yang ada dalam grup aturan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.4.1	Aplikasi web yang menghadap publik dilindungi dari serangan. (PCI-DSS-V4.0)	waf-global-rule-not-kosong	Pastikan bahwa aturan global AWS WAF berisi beberapa kondisi. Aturannya adalah NON_COMPLIANT jika tidak ada kondisi dalam aturan global WAF.
6.4.2	Aplikasi web yang menghadap publik dilindungi dari serangan. (PCI-DSS-V4.0)	cloudfront-associated-with-waf	Pastikan CloudFront distribusi Amazon dikaitkan dengan firewall aplikasi web (WAF) atau daftar kontrol akses WAFv2 web (ACLs). Aturannya adalah NON_COMPLIANT jika CloudFront distribusi tidak terkait dengan ACL web WAF.
6.4.2	Aplikasi web yang menghadap publik dilindungi dari serangan. (PCI-DSS-V4.0)	appsync-associated-with-waf	Pastikan AWS AppSync APIs yang terkait dengan daftar kontrol akses AWS WAFv2 web (ACLs). Aturannya adalah NON_COMPLIANT untuk AWS AppSync API jika tidak terkait dengan ACL web.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.4.2	Aplikasi web yang menghadap publik dilindungi dari serangan. (PCI-DSS-V4.0)	wafv2- webacl-not-empty	Pastikan bahwa ACL WAFv2 Web berisi aturan WAF atau grup aturan WAF. Aturan ini NON_COMPL IANT jika ACL Web tidak berisi aturan WAF atau grup aturan WAF.
6.4.2	Aplikasi web yang menghadap publik dilindungi dari serangan. (PCI-DSS-V4.0)	wafv2- rulegroup-not-empty	Pastikan bahwa Grup WAFv2 Aturan berisi aturan. Aturannya adalah NON_COMPL IANT jika tidak ada aturan dalam Grup Aturan. WAFv2
6.4.2	Aplikasi web yang menghadap publik dilindungi dari serangan. (PCI-DSS-V4.0)	waf-global-webacl-not-kosong	Pastikan bahwa WAF Global Web ACL berisi beberapa aturan WAF atau grup aturan. Aturan ini adalah NON_COMPL IANT jika ACL Web tidak berisi aturan WAF atau grup aturan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.4.2	Aplikasi web yang menghadap publik dilindungi dari serangan. (PCI-DSS-V4.0)	waf-global-rulegroup-not-kosong	Pastikan grup aturan AWS WAF Classic berisi beberapa aturan. Aturannya adalah NON_COMPLIANT jika tidak ada aturan yang ada dalam grup aturan.
6.4.2	Aplikasi web yang menghadap publik dilindungi dari serangan. (PCI-DSS-V4.0)	waf-global-rulegroup-not-kosong	Pastikan grup aturan AWS WAF Classic berisi beberapa aturan. Aturannya adalah NON_COMPLIANT jika tidak ada aturan yang ada dalam grup aturan.
6.4.2	Aplikasi web yang menghadap publik dilindungi dari serangan. (PCI-DSS-V4.0)	waf-global-rule-not-kosong	Pastikan bahwa aturan global AWS WAF berisi beberapa kondisi. Aturannya adalah NON_COMPLIANT jika tidak ada kondisi dalam aturan global WAF.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.5.5	Perubahan pada semua komponen sistem dikelola dengan aman. (PCI-DSS-V4.0)	codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan	Pastikan bahwa grup penyebara n untuk Lambda Compute Platform tidak menggunak an konfigurasi penerapan default. Aturannya adalah NON_COMPLIANT jika grup penerapan menggunakan konfigurasi penerapan '. CodeDeployDefault LambdaAllAtOnce'.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.5.5	Perubahan pada semua komponen sistem dikelola dengan aman. (PCI-DSS-V4.0)	codepipeline-deployment-count-check	Pastikan bahwa tahap penyebaran pertama AWS CodePipeline melakukan setidaknya satu penerapan. Ini untuk memantau aktivitas penyebaran berkelanjutan, memastikan pembaruan rutin dan mengidentifikasi saluran pipa yang tidak aktif atau kurang dimanfaatkan, yang dapat menandakan masalah dalam proses pengembangan atau penyebaran. Secara opsional memastikan bahwa setiap tahapan berikutnya yang tersisa disebarkan ke lebih dari jumlah penerapan yang ditentukan (deploymentLimit).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.5.6	Perubahan pada semua komponen sistem dikelola dengan aman. (PCI-DSS-V4.0)	codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan	Pastikan bahwa grup penyebaran untuk Lambda Compute Platform tidak menggunakan konfigurasi penerapan default. Aturannya adalah NON_COMPLIANT jika grup penerapan menggunakan konfigurasi penerapan '. CodeDeployDefaultLambdaAllAtOnce'.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.5.6	Perubahan pada semua komponen sistem dikelola dengan aman. (PCI-DSS-V4.0)	codepipeline-deployment-count-check	Pastikan bahwa tahap penyebaran pertama AWS CodePipeline melakukan setidaknya satu penerapan. Ini untuk memantau aktivitas penyebaran berkelanjutan, memastikan pembaruan rutin dan mengidentifikasi saluran pipa yang tidak aktif atau kurang dimanfaatkan, yang dapat menandakan masalah dalam proses pengembangan atau penyebaran. Secara opsional memastikan bahwa setiap tahapan berikutnya yang tersisa disebarkan ke lebih dari jumlah penerapan yang ditentukan (deploymentLimit).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.1	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	s3- bucket-blacklisted-actions-prohibited	Pastikan kebijakan bucket Amazon Simple Storage Service (Amazon S3) tidak mengizinkan tindakan tingkat ember dan tingkat objek yang diblokir pada sumber daya dalam bucket untuk prinsipal dari akun lain. AWS Misalnya, aturan memeriksa bahwa kebijakan bucket Amazon S3 tidak mengizinkan AWS akun lain untuk melakukan tindakan s3: GetBucket * dan s3: DeleteObject pada objek apa pun di bucket. Aturannya adalah NON_COMPLIANT jika ada tindakan yang diblokir yang diizinkan oleh kebijakan bucket Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.1	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	s3- bucket-policy-not-more -permisif	Pastikan kebijakan bucket Amazon Simple Storage Service (S3) Anda tidak mengizinkan izin antar akun selain kebijakan bucket Amazon S3 kontrol yang Anda berikan.
7.2.1	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	shield-drt-access	Pastikan bahwa Shield Response Team (SRT) dapat mengakses AWS akun Anda. Aturannya adalah NON_COMPL IANT jika AWS Shield Advanced diaktifka n tetapi peran untuk akses SRT tidak dikonfigurasi.
7.2.1	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	iam-policy-in-use	Pastikan bahwa ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.1	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	neptune-cluster-iam-database-otentikasi	Pastikan klaster AWS Amazon Neptune mengaktif kan otentikasi database Identity and Access Managemen t (IAM) and Access Management (IAM). Aturannya adalah NON_COMPL IANT jika klaster Amazon Neptunus tidak mengaktifkan autentikasi database IAM.
7.2.1	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	rds-cluster-iam-au thentication-diaktifkan	Pastikan klaster AWS Amazon Relational Database Service (Amazon RDS) mengaktif kan autentikasi Identity and Access Management (IAM). Aturannya adalah NON_COMPLIANT jika Cluster Amazon RDS tidak mengaktif kan autentikasi IAM.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.1	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	ec2- instance-profile-attached	Pastikan bahwa sebuah EC2 instans memiliki profil AWS Identity and Access Management (IAM) yang dilampirkan padanya. Aturannya adalah NON_COMPLIANT jika tidak ada profil IAM yang dilampirkan ke instance. EC2

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.1	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan brankas cadangan memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Aturannya adalah NON_COMPLIANT jika Brankas Cadangan tidak memiliki kebijakan berbasis sumber daya atau memiliki kebijakan tanpa pernyataan 'Deny' yang sesuai (pernyataan dengan cadangan: DeleteRecoveryPoint, cadangan:, dan cadangan: izin). UpdateRecoveryPointLifecycle PutBackupVaultAccessPolicy

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.1	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	rds-instance-iam-authentication-diaktifkan	Pastikan instans AWS Amazon Relational Database Service (Amazon RDS) mengaktifkan autentikasi Identity and Access Management (IAM). Aturannya adalah NON_COMPLIANT jika instans Amazon RDS tidak mengaktifkan autentikasi IAM.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.2	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	s3- bucket-blacklisted-actions-prohibited	Pastikan kebijakan bucket Amazon Simple Storage Service (Amazon S3) tidak mengizinkan tindakan tingkat ember dan tingkat objek yang diblokir pada sumber daya dalam bucket untuk prinsipal dari akun lain. AWS Misalnya, aturan memeriksa bahwa kebijakan bucket Amazon S3 tidak mengizinkan AWS akun lain untuk melakukan tindakan s3: GetBucket * dan s3: DeleteObject pada objek apa pun di bucket. Aturannya adalah NON_COMPLIANT jika ada tindakan yang diblokir yang diizinkan oleh kebijakan bucket Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.2	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	s3- bucket-policy-not-more -permisif	Pastikan kebijakan bucket Amazon Simple Storage Service (S3) Anda tidak mengizinkan izin antar akun selain kebijakan bucket Amazon S3 kontrol yang Anda berikan.
7.2.2	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	shield-drt-access	Pastikan bahwa Shield Response Team (SRT) dapat mengakses AWS akun Anda. Aturannya adalah NON_COMPLIANT jika AWS Shield Advanced diaktifkan tetapi peran untuk akses SRT tidak dikonfigurasi.
7.2.2	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	iam-policy-in-use	Pastikan bahwa ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.2	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	neptune-cluster-iam-database-otentikasi	Pastikan klaster AWS Amazon Neptune mengaktif kan otentikasi database Identity and Access Managemen t (IAM) and Access Management (IAM). Aturannya adalah NON_COMPL IANT jika klaster Amazon Neptunus tidak mengaktifkan autentikasi database IAM.
7.2.2	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	rds-cluster-iam-au thentication-diaktifkan	Pastikan klaster AWS Amazon Relational Database Service (Amazon RDS) mengaktif kan autentikasi Identity and Access Management (IAM). Aturannya adalah NON_COMPLIANT jika Cluster Amazon RDS tidak mengaktif kan autentikasi IAM.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.2	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	ec2- instance-profile-attached	Pastikan bahwa sebuah EC2 instans memiliki profil AWS Identity and Access Management (IAM) yang dilampirkan padanya. Aturannya adalah NON_COMPLIANT jika tidak ada profil IAM yang dilampirkan ke instance. EC2

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.2	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan brankas cadangan memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Aturannya adalah NON_COMPLIANT jika Brankas Cadangan tidak memiliki kebijakan berbasis sumber daya atau memiliki kebijakan tanpa pernyataan 'Deny' yang sesuai (pernyataan dengan cadangan: DeleteRecoveryPoint, cadangan:, dan cadangan: izin). UpdateRecoveryPointLifecycle PutBackupVaultAccessPolicy

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.2	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	rds-instance-iam-authentication-diaktifkan	Pastikan instans AWS Amazon Relational Database Service (Amazon RDS) mengaktif kan autentikasi Identity and Access Management (IAM). Aturannya adalah NON_COMPLIANT jika instans Amazon RDS tidak mengaktif kan autentikasi IAM.
7.2.4	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	secretsmanager-secret-unused	Pastikan AWS rahasia Secrets Manager telah diakses dalam beberapa hari tertentu. Aturannya adalah NON_COMPLIANT jika rahasia belum diakses dalam jumlah hari unusedForDays ". Nilai defaultnya adalah 90 hari.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.5	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	s3- bucket-blacklisted-actions-prohibited	Pastikan kebijakan bucket Amazon Simple Storage Service (Amazon S3) tidak mengizinkan tindakan tingkat ember dan tingkat objek yang diblokir pada sumber daya dalam bucket untuk prinsipal dari akun lain. AWS Misalnya, aturan memeriksa bahwa kebijakan bucket Amazon S3 tidak mengizinkan AWS akun lain untuk melakukan tindakan s3: GetBucket * dan s3: DeleteObject pada objek apa pun di bucket. Aturannya adalah NON_COMPLIANT jika ada tindakan yang diblokir yang diizinkan oleh kebijakan bucket Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.5	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	s3- bucket-policy-not-more -permisif	Pastikan kebijakan bucket Amazon Simple Storage Service (S3) Anda tidak mengizinkan izin antar akun selain kebijakan bucket Amazon S3 kontrol yang Anda berikan.
7.2.5	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	shield-drt-access	Pastikan bahwa Shield Response Team (SRT) dapat mengakses AWS akun Anda. Aturannya adalah NON_COMPL IANT jika AWS Shield Advanced diaktifka n tetapi peran untuk akses SRT tidak dikonfigurasi.
7.2.5	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	iam-policy-in-use	Pastikan bahwa ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.5	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	neptune-cluster-iam-database-otentikasi	Pastikan klaster AWS Amazon Neptune mengaktif kan otentikasi database Identity and Access Managemen t (IAM) and Access Management (IAM). Aturannya adalah NON_COMPL IANT jika klaster Amazon Neptunus tidak mengaktifkan autentikasi database IAM.
7.2.5	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	rds-cluster-iam-au thentication-diaktifkan	Pastikan klaster AWS Amazon Relational Database Service (Amazon RDS) mengaktif kan autentikasi Identity and Access Management (IAM). Aturannya adalah NON_COMPLIANT jika Cluster Amazon RDS tidak mengaktif kan autentikasi IAM.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.5	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	ec2- instance-profile-attached	Pastikan bahwa sebuah EC2 instans memiliki profil AWS Identity and Access Management (IAM) yang dilampirkan padanya. Aturannya adalah NON_COMPLIANT jika tidak ada profil IAM yang dilampirkan ke instance. EC2

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.5	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan brankas cadangan memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Aturannya adalah NON_COMPLIANT jika Brankas Cadangan tidak memiliki kebijakan berbasis sumber daya atau memiliki kebijakan tanpa pernyataan 'Deny' yang sesuai (pernyataan dengan cadangan: DeleteRecoveryPoint, cadangan:, dan cadangan: izin). UpdateRecoveryPointLifecycle PutBackupVaultAccessPolicy

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.5	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	rds-instance-iam-authentication-diaktifkan	Pastikan instans AWS Amazon Relational Database Service (Amazon RDS) mengaktif kan autentikasi Identity and Access Management (IAM). Aturannya adalah NON_COMPLIANT jika instans Amazon RDS tidak mengaktif kan autentikasi IAM.
7.2.5.1	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	secretsmanager-secret-unused	Pastikan AWS rahasia Secrets Manager telah diakses dalam beberapa hari tertentu. Aturannya adalah NON_COMPLIANT jika rahasia belum diakses dalam jumlah hari unusedFor Days ". Nilai defaultnya adalah 90 hari.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.6	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	s3- bucket-blacklisted-actions-prohibited	Pastikan kebijakan bucket Amazon Simple Storage Service (Amazon S3) tidak mengizinkan tindakan tingkat ember dan tingkat objek yang diblokir pada sumber daya dalam bucket untuk prinsipal dari akun lain. AWS Misalnya, aturan memeriksa bahwa kebijakan bucket Amazon S3 tidak mengizinkan AWS akun lain untuk melakukan tindakan s3: GetBucket * dan s3: DeleteObject pada objek apa pun di bucket. Aturannya adalah NON_COMPLIANT jika ada tindakan yang diblokir yang diizinkan oleh kebijakan bucket Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.2.6	Akses ke komponen dan data sistem didefinisikan dan ditetapkan dengan tepat. (PCI-DSS-V4.0)	s3- bucket-policy-not-more -permisif	Pastikan kebijakan bucket Amazon Simple Storage Service (S3) Anda tidak mengizinkan izin antar akun selain kebijakan bucket Amazon S3 kontrol yang Anda berikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.1	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	s3- bucket-blacklisted-actions-prohibited	Pastikan kebijakan bucket Amazon Simple Storage Service (Amazon S3) tidak mengizinkan tindakan tingkat ember dan tingkat objek yang diblokir pada sumber daya dalam bucket untuk prinsipal dari akun lain. AWS Misalnya, aturan memeriksa bahwa kebijakan bucket Amazon S3 tidak mengizinkan AWS akun lain untuk melakukan tindakan s3: GetBucket * dan s3: DeleteObject pada objek apa pun di bucket. Aturannya adalah NON_COMPLIANT jika ada tindakan yang diblokir yang diizinkan oleh kebijakan bucket Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.1	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	s3- bucket-policy-not-more -permisif	Pastikan kebijakan bucket Amazon Simple Storage Service (S3) Anda tidak mengizinkan izin antar akun selain kebijakan bucket Amazon S3 kontrol yang Anda berikan.
7.3.1	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	shield-drt-access	Pastikan bahwa Shield Response Team (SRT) dapat mengakses AWS akun Anda. Aturannya adalah NON_COMPLIANT jika AWS Shield Advanced diaktifkan tetapi peran untuk akses SRT tidak dikonfigurasi.
7.3.1	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	iam-policy-in-use	Pastikan bahwa ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.1	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	neptune-cluster-iam-database-otentikasi	Pastikan klaster AWS Amazon Neptune mengaktif kan otentikasi database Identity and Access Managemen t (IAM) and Access Management (IAM). Aturannya adalah NON_COMPL IANT jika klaster Amazon Neptunus tidak mengaktifkan autentikasi database IAM.
7.3.1	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	rds-cluster-iam-au thentication-diaktifkan	Pastikan klaster AWS Amazon Relational Database Service (Amazon RDS) mengaktif kan autentikasi Identity and Access Management (IAM). Aturannya adalah NON_COMPLIANT jika Cluster Amazon RDS tidak mengaktif kan autentikasi IAM.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.1	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	ec2- instance-profile-attached	Pastikan bahwa sebuah EC2 instans memiliki profil AWS Identity and Access Management (IAM) yang dilampirkan padanya. Aturannya adalah NON_COMPLIANT jika tidak ada profil IAM yang dilampirkan ke instance. EC2

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.1	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan brankas cadangan memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Aturannya adalah NON_COMPLIANT jika Brankas Cadangan tidak memiliki kebijakan berbasis sumber daya atau memiliki kebijakan tanpa pernyataan 'Deny' yang sesuai (pernyataan dengan cadangan: DeleteRecoveryPoint, cadangan:, dan cadangan: izin). UpdateRecoveryPointLifecycle PutBackupVaultAccessPolicy

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.1	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	rds-instance-iam-authentication-diaktifkan	Pastikan instans AWS Amazon Relational Database Service (Amazon RDS) mengaktifkan autentikasi Identity and Access Management (IAM). Aturannya adalah NON_COMPLIANT jika instans Amazon RDS tidak mengaktifkan autentikasi IAM.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.2	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	s3- bucket-blacklisted-actions-prohibited	Pastikan kebijakan bucket Amazon Simple Storage Service (Amazon S3) tidak mengizinkan tindakan tingkat ember dan tingkat objek yang diblokir pada sumber daya dalam bucket untuk prinsipal dari akun lain. AWS Misalnya, aturan memeriksa bahwa kebijakan bucket Amazon S3 tidak mengizinkan AWS akun lain untuk melakukan tindakan s3: GetBucket * dan s3: DeleteObject pada objek apa pun di bucket. Aturannya adalah NON_COMPLIANT jika ada tindakan yang diblokir yang diizinkan oleh kebijakan bucket Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.2	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	s3- bucket-policy-not-more -permisif	Pastikan kebijakan bucket Amazon Simple Storage Service (S3) Anda tidak mengizinkan izin antar akun selain kebijakan bucket Amazon S3 kontrol yang Anda berikan.
7.3.2	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	shield-drt-access	Pastikan bahwa Shield Response Team (SRT) dapat mengakses AWS akun Anda. Aturannya adalah NON_COMPLIANT jika AWS Shield Advanced diaktifkan tetapi peran untuk akses SRT tidak dikonfigurasi.
7.3.2	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	iam-policy-in-use	Pastikan bahwa ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.2	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	neptune-cluster-iam-database-otentikasi	Pastikan klaster AWS Amazon Neptune mengaktif kan otentikasi database Identity and Access Managemen t (IAM) and Access Management (IAM). Aturannya adalah NON_COMPL IANT jika klaster Amazon Neptunus tidak mengaktifkan autentikasi database IAM.
7.3.2	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	rds-cluster-iam-au thentication-diaktifkan	Pastikan klaster AWS Amazon Relational Database Service (Amazon RDS) mengaktif kan autentikasi Identity and Access Management (IAM). Aturannya adalah NON_COMPLIANT jika Cluster Amazon RDS tidak mengaktif kan autentikasi IAM.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.2	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	ec2- instance-profile-attached	Pastikan bahwa sebuah EC2 instans memiliki profil AWS Identity and Access Management (IAM) yang dilampirkan padanya. Aturannya adalah NON_COMPLIANT jika tidak ada profil IAM yang dilampirkan ke instance. EC2

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.2	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan brankas cadangan memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Aturannya adalah NON_COMPLIANT jika Brankas Cadangan tidak memiliki kebijakan berbasis sumber daya atau memiliki kebijakan tanpa pernyataan 'Deny' yang sesuai (pernyataan dengan cadangan: DeleteRecoveryPoint, cadangan:, dan cadangan: izin). UpdateRecoveryPointLifecycle PutBackupVaultAccessPolicy

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.2	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	rds-instance-iam-authentication-diaktifkan	Pastikan instans AWS Amazon Relational Database Service (Amazon RDS) mengaktifkan autentikasi Identity and Access Management (IAM). Aturannya adalah NON_COMPLIANT jika instans Amazon RDS tidak mengaktifkan autentikasi IAM.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.3	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	s3- bucket-blacklisted-actions-prohibited	Pastikan kebijakan bucket Amazon Simple Storage Service (Amazon S3) tidak mengizinkan tindakan tingkat ember dan tingkat objek yang diblokir pada sumber daya dalam bucket untuk prinsipal dari akun lain. AWS Misalnya, aturan memeriksa bahwa kebijakan bucket Amazon S3 tidak mengizinkan AWS akun lain untuk melakukan tindakan s3: GetBucket * dan s3: DeleteObject pada objek apa pun di bucket. Aturannya adalah NON_COMPLIANT jika ada tindakan yang diblokir yang diizinkan oleh kebijakan bucket Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.3	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	s3- bucket-policy-not-more -permisif	Pastikan kebijakan bucket Amazon Simple Storage Service (S3) Anda tidak mengizinkan izin antar akun selain kebijakan bucket Amazon S3 kontrol yang Anda berikan.
7.3.3	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	shield-drt-access	Pastikan bahwa Shield Response Team (SRT) dapat mengakses AWS akun Anda. Aturannya adalah NON_COMPLIANT jika AWS Shield Advanced diaktifkan tetapi peran untuk akses SRT tidak dikonfigurasi.
7.3.3	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	iam-policy-in-use	Pastikan bahwa ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.3	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	neptune-cluster-iam-database-otentikasi	Pastikan klaster AWS Amazon Neptune mengaktif kan otentikasi database Identity and Access Managemen t (IAM) and Access Management (IAM). Aturannya adalah NON_COMPL IANT jika klaster Amazon Neptunus tidak mengaktifkan autentikasi database IAM.
7.3.3	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	rds-cluster-iam-au thentication-diaktifkan	Pastikan klaster AWS Amazon Relational Database Service (Amazon RDS) mengaktif kan autentikasi Identity and Access Management (IAM). Aturannya adalah NON_COMPLIANT jika Cluster Amazon RDS tidak mengaktif kan autentikasi IAM.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.3	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	ec2- instance-profile-attached	Pastikan bahwa sebuah EC2 instans memiliki profil AWS Identity and Access Management (IAM) yang dilampirkan padanya. Aturannya adalah NON_COMPLIANT jika tidak ada profil IAM yang dilampirkan ke instance. EC2

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.3	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan brankas cadangan memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Aturannya adalah NON_COMPLIANT jika Brankas Cadangan tidak memiliki kebijakan berbasis sumber daya atau memiliki kebijakan tanpa pernyataan 'Deny' yang sesuai (pernyataan dengan cadangan: DeleteRecoveryPoint, cadangan:, dan cadangan: izin). UpdateRecoveryPointLifecycle PutBackupVaultAccessPolicy

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
7.3.3	Akses ke komponen sistem dan data dikelola melalui sistem kontrol akses. (PCI-DSS-V4.0)	rds-instance-iam-authentication-diaktifkan	Pastikan instans AWS Amazon Relational Database Service (Amazon RDS) mengaktifkan autentikasi Identity and Access Management (IAM). Aturannya adalah NON_COMPLIANT jika instans Amazon RDS tidak mengaktifkan autentikasi IAM.
8.2.1	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	iam-policy-in-use	Pastikan bahwa ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.1	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	ec2- no-amazon-key-pair	Pastikan instans Amazon Elastic Compute Cloud (EC2) yang menjalank an tidak diluncurk an menggunakan pasangan kunci amazon. Aturannya adalah NON_COMPL IANT jika EC2 instance yang sedang berjalan diluncurkan dengan key pair.
8.2.2	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	iam-policy-in-use	Pastikan bahwa ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.2	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	ec2- no-amazon-key-pair	Pastikan instans Amazon Elastic Compute Cloud (EC2) yang menjalankan tidak diluncurkan menggunakan pasangan kunci amazon. Aturannya adalah NON_COMPLIANT jika EC2 instance yang sedang berjalan diluncurkan dengan key pair.
8.2.2	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	codebuild-project-envvar-awscred-periksa	Pastikan bahwa proyek TIDAK berisi variabel lingkungan AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY. Aturannya adalah NON_COMPLIANT ketika variabel lingkungan proyek berisi kredenal teks biasa.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.2	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	secretsmanager-scheduled-rotation-success-periksa	Pastikan AWS rahasia Secrets Manager diputar dengan sukses sesuai dengan jadwal rotasi. Secrets Manager menghitung tanggal rotasi harus terjadi. Aturannya adalah NON_COMPLIANT jika tanggal berlalu dan rahasianya tidak diputar.
8.2.2	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	secretsmanager-secret-periodic-rotation	Pastikan AWS rahasia Secrets Manager telah dirotasi dalam jumlah hari yang ditentukan sebelumnya. Aturannya adalah NON_COMPLIANT jika rahasia belum diputar selama lebih dari jumlah hari maxDaysSinceRotasi. Nilai defaultnya adalah 90 hari.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.2	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	secretsmanager-secret-unused	Pastikan AWS rahasia Secrets Manager telah diakses dalam beberapa hari tertentu. Aturannya adalah NON_COMPLIANT jika rahasia belum diakses dalam jumlah hari unusedForDays ". Nilai defaultnya adalah 90 hari.
8.2.4	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	iam-policy-in-use	Pastikan bahwa ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.4	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	ec2- no-amazon-key-pair	Pastikan instans Amazon Elastic Compute Cloud (EC2) yang menjalank an tidak diluncurk an menggunakan pasangan kunci amazon. Aturannya adalah NON_COMPL IANT jika EC2 instance yang sedang berjalan diluncurkan dengan key pair.
8.2.5	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	iam-policy-in-use	Pastikan bahwa ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.5	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	ec2- no-amazon-key-pair	Pastikan instans Amazon Elastic Compute Cloud (EC2) yang menjalank an tidak diluncurk an menggunakan pasangan kunci amazon. Aturannya adalah NON_COMPL IANT jika EC2 instance yang sedang berjalan diluncurkan dengan key pair.
8.2.6	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	secretsmanager-sec ret-unused	Pastikan AWS rahasia Secrets Manager telah diakses dalam beberapa hari tertentu. Aturannya adalah NON_COMPL IANT jika rahasia belum diakses dalam jumlah hari unusedFor Days ". Nilai defaultny a adalah 90 hari.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.7	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	s3- bucket-blacklisted-actions-prohibited	Pastikan kebijakan bucket Amazon Simple Storage Service (Amazon S3) tidak mengizinkan tindakan tingkat ember dan tingkat objek yang diblokir pada sumber daya dalam bucket untuk prinsipal dari akun lain. AWS Misalnya, aturan memeriksa bahwa kebijakan bucket Amazon S3 tidak mengizinkan AWS akun lain untuk melakukan tindakan s3: GetBucket * dan s3: DeleteObject pada objek apa pun di bucket. Aturannya adalah NON_COMPLIANT jika ada tindakan yang diblokir yang diizinkan oleh kebijakan bucket Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.7	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	s3- bucket-policy-not-more -permisif	Pastikan kebijakan bucket Amazon Simple Storage Service (S3) Anda tidak mengizinkan izin antar akun selain kebijakan bucket Amazon S3 kontrol yang Anda berikan.
8.2.7	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	shield-drt-access	Pastikan bahwa Shield Response Team (SRT) dapat mengakses AWS akun Anda. Aturannya adalah NON_COMPLIANT jika AWS Shield Advanced diaktifkan tetapi peran untuk akses SRT tidak dikonfigurasi.
8.2.7	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	iam-policy-in-use	Pastikan bahwa ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.7	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	neptune-cluster-iam-database-otentikasi	Pastikan klaster AWS Amazon Neptune mengaktif kan otentikasi database Identity and Access Managemen t (IAM) and Access Management (IAM). Aturannya adalah NON_COMPL IANT jika klaster Amazon Neptunus tidak mengaktifkan autentikasi database IAM.
8.2.7	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	rds-cluster-iam-au thentication-diaktifkan	Pastikan klaster AWS Amazon Relational Database Service (Amazon RDS) mengaktif kan autentikasi Identity and Access Management (IAM). Aturannya adalah NON_COMPLIANT jika Cluster Amazon RDS tidak mengaktif kan autentikasi IAM.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.7	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	ec2- instance-profile-attached	Pastikan bahwa sebuah EC2 instans memiliki profil AWS Identity and Access Management (IAM) yang dilampirkan padanya. Aturannya adalah NON_COMPLIANT jika tidak ada profil IAM yang dilampirkan ke instance. EC2

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.7	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan brankas cadangan memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Aturannya adalah NON_COMPLIANT jika Brankas Cadangan tidak memiliki kebijakan berbasis sumber daya atau memiliki kebijakan tanpa pernyataan 'Deny' yang sesuai (pernyataan dengan cadangan: DeleteRecoveryPoint, cadangan:, dan cadangan: izin). UpdateRecoveryPointLifecycle PutBackupVaultAccessPolicy

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.7	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	rds-instance-iam-authentication-diaktifkan	Pastikan instans AWS Amazon Relational Database Service (Amazon RDS) mengaktifkan autentikasi Identity and Access Management (IAM). Aturannya adalah NON_COMPLIANT jika instans Amazon RDS tidak mengaktifkan autentikasi IAM.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.8	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	s3- bucket-blacklisted-actions-prohibited	Pastikan kebijakan bucket Amazon Simple Storage Service (Amazon S3) tidak mengizinkan tindakan tingkat ember dan tingkat objek yang diblokir pada sumber daya dalam bucket untuk prinsipal dari akun lain. AWS Misalnya, aturan memeriksa bahwa kebijakan bucket Amazon S3 tidak mengizinkan AWS akun lain untuk melakukan tindakan s3: GetBucket * dan s3: DeleteObject pada objek apa pun di bucket. Aturannya adalah NON_COMPLIANT jika ada tindakan yang diblokir yang diizinkan oleh kebijakan bucket Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.8	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	s3- bucket-policy-not-more -permisif	Pastikan kebijakan bucket Amazon Simple Storage Service (S3) Anda tidak mengizinkan izin antar akun selain kebijakan bucket Amazon S3 kontrol yang Anda berikan.
8.2.8	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	shield-drt-access	Pastikan bahwa Shield Response Team (SRT) dapat mengakses AWS akun Anda. Aturannya adalah NON_COMPLIANT jika AWS Shield Advanced diaktifkan tetapi peran untuk akses SRT tidak dikonfigurasi.
8.2.8	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	iam-policy-in-use	Pastikan bahwa ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.8	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	neptune-cluster-iam-database-otentikasi	Pastikan klaster AWS Amazon Neptune mengaktif kan otentikasi database Identity and Access Managemen t (IAM) and Access Management (IAM). Aturannya adalah NON_COMPL IANT jika klaster Amazon Neptunus tidak mengaktifkan autentikasi database IAM.
8.2.8	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	rds-cluster-iam-au thentication-diaktifkan	Pastikan klaster AWS Amazon Relational Database Service (Amazon RDS) mengaktif kan autentikasi Identity and Access Management (IAM). Aturannya adalah NON_COMPLIANT jika Cluster Amazon RDS tidak mengaktif kan autentikasi IAM.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.8	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	ec2-imdsv2-periksa	Pastikan versi metadata instans Amazon Elastic Compute Cloud (Amazon EC2) Anda dikonfigurasi dengan Instance Metadata Service Version 2 (). IMDSv2 Aturannya adalah NON_COMPLIANT jika HttpTokens disetel ke opsional.
8.2.8	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	ec2- instance-profile-attached	Pastikan bahwa sebuah EC2 instans memiliki profil AWS Identity and Access Management (IAM) yang dilampirkan padanya. Aturannya adalah NON_COMPLIANT jika tidak ada profil IAM yang dilampirkan ke instance. EC2

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.8	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	autoscaling-launchconfig-requires-imdsv2	Pastikan bahwa hanya IMDSv2 diaktifkan. Aturan ini NON_COMPLIANT jika versi Metadata tidak disertakan dalam konfigurasi peluncuran atau jika kedua Metadata V1 dan V2 diaktifkan.
8.2.8	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan brankas cadangan memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Aturannya adalah NON_COMPLIANT jika Brankas Cadangan tidak memiliki kebijakan berbasis sumber daya atau memiliki kebijakan tanpa pernyataan 'Deny' yang sesuai (pernyataan dengan cadangan: DeleteRecoveryPoint, cadangan:, dan cadangan: izin). UpdateRecoveryPointLifecycle PutBackupVaultAccessPolicy

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.2.8	Identifikasi pengguna dan akun terkait untuk pengguna dan administrator dikelola secara ketat sepanjang siklus hidup akun. (PCI-DSS-V4.0)	rds-instance-iam-authentication-diaktifkan	Pastikan instans AWS Amazon Relational Database Service (Amazon RDS) mengaktifkan autentikasi Identity and Access Management (IAM). Aturannya adalah NON_COMPLIANT jika instans Amazon RDS tidak mengaktifkan autentikasi IAM.
8.3.10.1	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	access-keys-rotated	Pastikan kunci akses IAM aktif diputar (diubah) dalam jumlah hari yang ditentukan dalam maxAccessKeyUsia. Aturannya adalah NON_COMPLIANT jika kunci akses tidak diputar dalam jangka waktu yang ditentukan. Nilai defaultnya adalah 90 hari.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.10.1	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	secretsmanager-scheduled-rotation-success-periksa	Pastikan AWS rahasia Secrets Manager diputar dengan sukses sesuai dengan jadwal rotasi. Secrets Manager menghitung tanggal rotasi harus terjadi. Aturannya adalah NON_COMPLIANT jika tanggal berlalu dan rahasianya tidak diputar.
8.3.10.1	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	secretsmanager-secret-periodic-rotation	Pastikan AWS rahasia Secrets Manager telah dirotasi dalam jumlah hari yang ditentukan sebelumnya. Aturannya adalah NON_COMPLIANT jika rahasia belum diputar selama lebih dari jumlah hari maxDaysSinceRotasi. Nilai defaultnya adalah 90 hari.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.11	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	iam-policy-in-use	Pastikan bahwa ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.
8.3.11	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	ec2- no-amazon-key-pair	Pastikan instans Amazon Elastic Compute Cloud (EC2) yang menjalank an tidak diluncurk an menggunakan pasangan kunci amazon. Aturannya adalah NON_COMPL IANT jika EC2 instance yang sedang berjalan diluncurkan dengan key pair.
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	athena-workgroup-e ncrypted-at-istirahat	Pastikan bahwa workgroup Amazon Athena dienkripsi saat istirahat. Aturannya adalah NON_COMPL IANT jika enkripsi data saat istirahat tidak diaktifkan untuk workgroup Athena.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	neptune-cluster-snapshot-encrypted	Pastikan bahwa kluster Amazon Neptunus DB memiliki snapshot yang dienkripsi. Aturannya adalah NON_COMPLIANT jika cluster Neptunus tidak memiliki snapshot yang dienkripsi.
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	redshift-cluster-kms-enabled	Pastikan klaster Amazon Redshift menggunakan AWS kunci Key Management Service (AWS KMS) yang ditentukan untuk enkripsi. Aturannya adalah COMPLIANT jika enkripsi diaktifkan dan cluster dienkripsi dengan kunci yang disediakan dalam parameter. kmsKeyArn Aturannya adalah NON_COMPLIANT jika cluster tidak dienkripsi atau dienkripsi dengan kunci lain.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	codebuild-project-artifact-encryption	Pastikan bahwa sebuah AWS CodeBuild proyek telah mengaktifkan enkripsi untuk semua artefaknya. Aturannya adalah NON_COMPLIANT jika 'EncryptionDisabled' disetel ke 'true' untuk konfigurasi artefak primer atau sekunder (jika ada).
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	codebuild-project-s3-log-terenkripsi	Pastikan AWS CodeBuild proyek yang dikonfigurasi dengan Amazon S3 Logs mengaktifkan enkripsi untuk lognya. Aturannya adalah NON_COMPLIANT jika 'EncryptionDisabled' disetel ke 'true' di S3 proyek. LogsConfig CodeBuild
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	dax-encryption-enabled	Pastikan klaster Amazon DynamoDB Accelerator (DAX) dienkripsi. Aturannya adalah NON_COMPLIANT jika cluster DAX tidak dienkripsi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	dms-redis-tls-enabled	Pastikan titik akhir AWS Database Migration Service (AWS DMS) untuk penyimpanan data Redis diaktifkan untuk TLS/SSL encryption of data communicated with other endpoints. The rule is NON_COMPLIANT if TLS/SSL enkripsi tidak diaktifkan.
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	eks-secrets-encrypted	Pastikan bahwa klaster Amazon Elastic Kubernetes Service dikonfigurasi agar rahasia Kubernetes dienkripsi menggunakan kunci Key Management Service (KMS). AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	api-gw-cache-enabled-dan-dienkripsi	Pastikan bahwa semua metode dalam tahapan Amazon API Gateway telah mengaktifkan cache dan cache dienkripsi. Aturannya adalah NON_COMPLIANT jika metode apa pun dalam tahap Amazon API Gateway tidak dikonfigurasi ke cache atau cache tidak dienkripsi.
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	docdb-cluster-encrypted	Pastikan enkripsi penyimpanan diaktifkan untuk klaster Amazon DocumentDB Anda (dengan kompatibilitas MongoDB). Aturannya adalah NON_COMPLIANT jika enkripsi penyimpanan tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	dynamodb-table-encrypted-kms	Pastikan tabel Amazon DynamoDB dienkripsi AWS dengan Key Management Service (KMS). Aturannya adalah NON_COMPLIANT jika tabel Amazon DynamoDB tidak dienkripsi dengan KMS. AWS Aturannya juga NON_COMPLIANT jika kunci AWS KMS terenkripsi tidak ada dalam parameter input. kmsKeyArns
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	dynamodb-table-encryption-enabled	Pastikan tabel Amazon DynamoDB dienkripsi dan memeriksa statusnya. Aturannya SESUAI jika status diaktifkan atau diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	cloudfront-no-deprecated-ssl-protokol	Pastikan CloudFront distribusi tidak menggunakan protokol SSL yang tidak digunakan lagi untuk komunikasi HTTPS antara lokasi tepi dan asal kustom. CloudFront Aturan ini adalah NON_COMPLIANT untuk CloudFront distribusi jika ada 'termasuk'. OriginSslProtocols SSLv3
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	cloudfront-traffic-to-origin-dienkripsi	Pastikan CloudFront distribusi Amazon mengenkripsi lalu lintas ke asal kustom. Aturannya adalah NON_COMPLIANT jika '' is'http-only' atau jika' 'adalah OriginProtocolPolicy 'match-viewer' dan' 'allow-all'. OriginProtocolPolicy ViewerProtocolPolicy

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	cloudfront-viewer-policy-https	Pastikan CloudFront distribusi Amazon Anda menggunakan HTTPS (secara langsung atau melalui pengalihan). Aturannya adalah NON_COMPLIANT jika nilai ViewerProtocolPolicy disetel ke 'allow-all' untuk atau untuk. DefaultCacheBehavior CacheBehaviors
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	codebuild-project-envvar-awscred-periksa	Pastikan bahwa proyek TIDAK berisi variabel lingkungan AWS_ACCESS_KEY_ID dan AWS_SECRET_ACCESS_KEY. Aturannya adalah NON_COMPLIANT ketika variabel lingkungan proyek berisi kredenal teks biasa.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancers . Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	dax-tls-endpoint-encryption	Pastikan klaster Amazon DynamoDB Accelerator (DAX) Anda telah disetel ke TLS. ClusterEndpointEncryptionType Aturannya adalah NON_COMPLIANT jika cluster DAX tidak dienkripsi oleh transport layer security (TLS).

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	eks-cluster-secrets-encrypted	Pastikan bahwa klaster Amazon EKS tidak dikonfigurasi agar rahasia Kubernetes dienkripsi menggunakan KMS. AWS Aturannya adalah NON_COMPLIANT jika kluster EKS tidak memiliki sumber daya EncryptionConfig atau jika EncryptionConfig tidak menyebutkan rahasia sebagai sumber daya.
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	kinesis-stream-encrypted	Pastikan aliran Amazon Kinesis dienkripsi saat istirahat dengan enkripsi sisi server. Aturannya adalah NON_COMPLIANT untuk aliran Kinesis jika " StreamEncryption tidak ada.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	msk-in-cluster-node-membutuhkan-tls	Pastikan bahwa klaster MSK Amazon memberlakukan enkripsi dalam perjalanan menggunakan HTTPS (TLS) dengan node broker klaster. Aturannya adalah NON_COMPLIANT jika komunikasi teks biasa diaktifkan untuk koneksi node broker in-cluster.
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	neptune-cluster-encrypted	Pastikan enkripsi penyimpanan diaktifkan untuk kluster Amazon Neptunus DB Anda. Aturannya adalah NON_COMPLIANT jika enkripsi penyimpanan tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.2	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	dms-endpoint-ssl-configured	Pastikan titik akhir AWS Database Migration Service (AWS DMS) dikonfigurasi dengan koneksi SSL. Aturannya adalah NON_COMPLIANT jika AWS DMS tidak memiliki koneksi SSL yang dikonfigurasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.4	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	s3- bucket-blacklisted-actions-prohibited	Pastikan kebijakan bucket Amazon Simple Storage Service (Amazon S3) tidak mengizinkan tindakan tingkat ember dan tingkat objek yang diblokir pada sumber daya dalam bucket untuk prinsipal dari akun lain. AWS Misalnya, aturan memeriksa bahwa kebijakan bucket Amazon S3 tidak mengizinkan AWS akun lain untuk melakukan tindakan s3: GetBucket * dan s3: DeleteObject pada objek apa pun di bucket. Aturannya adalah NON_COMPLIANT jika ada tindakan yang diblokir yang diizinkan oleh kebijakan bucket Amazon S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.4	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	s3- bucket-policy-not-more -permisif	Pastikan kebijakan bucket Amazon Simple Storage Service (S3) Anda tidak mengizinkan izin antar akun selain kebijakan bucket Amazon S3 kontrol yang Anda berikan.
8.3.4	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	shield-drt-access	Pastikan bahwa Shield Response Team (SRT) dapat mengakses AWS akun Anda. Aturannya adalah NON_COMPLIANT jika AWS Shield Advanced diaktifkan tetapi peran untuk akses SRT tidak dikonfigurasi.
8.3.4	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	iam-policy-in-use	Pastikan bahwa ARN kebijakan IAM dilampirkan ke pengguna IAM, atau grup dengan satu atau lebih pengguna IAM, atau peran IAM dengan satu atau lebih entitas tepercaya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.4	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	neptune-cluster-iam-database-otentikasi	Pastikan klaster AWS Amazon Neptune mengaktif kan otentikasi database Identity and Access Managemen t (IAM) and Access Management (IAM). Aturannya adalah NON_COMPL IANT jika klaster Amazon Neptunus tidak mengaktifkan autentikasi database IAM.
8.3.4	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	rds-cluster-iam-au thentication-diaktifkan	Pastikan klaster AWS Amazon Relational Database Service (Amazon RDS) mengaktif kan autentikasi Identity and Access Management (IAM). Aturannya adalah NON_COMPLIANT jika Cluster Amazon RDS tidak mengaktif kan autentikasi IAM.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.4	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	ec2- instance-profile-attached	Pastikan bahwa sebuah EC2 instans memiliki profil AWS Identity and Access Management (IAM) yang dilampirkan padanya. Aturannya adalah NON_COMPLIANT jika tidak ada profil IAM yang dilampirkan ke instance. EC2

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.4	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan brankas cadangan memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Aturannya adalah NON_COMPLIANT jika Brankas Cadangan tidak memiliki kebijakan berbasis sumber daya atau memiliki kebijakan tanpa pernyataan 'Deny' yang sesuai (pernyataan dengan cadangan: DeleteRecoveryPoint, cadangan:, dan cadangan: izin). UpdateRecoveryPointLifecycle PutBackupVaultAccessPolicy

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.4	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	rds-instance-iam-authentication-diaktifkan	Pastikan instans AWS Amazon Relational Database Service (Amazon RDS) mengaktifkan autentikasi Identity and Access Management (IAM). Aturannya adalah NON_COMPLIANT jika instans Amazon RDS tidak mengaktifkan autentikasi IAM.
8.3.5	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	access-keys-rotated	Pastikan kunci akses IAM aktif diputar (diubah) dalam jumlah hari yang ditentukan dalam maxAccessKeyUsia. Aturannya adalah NON_COMPLIANT jika kunci akses tidak diputar dalam jangka waktu yang ditentukan. Nilai defaultnya adalah 90 hari.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.5	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	secretsmanager-scheduled-rotation-success-periksa	Pastikan AWS rahasia Secrets Manager diputar dengan sukses sesuai dengan jadwal rotasi. Secrets Manager menghitung tanggal rotasi harus terjadi. Aturannya adalah NON_COMPLIANT jika tanggal berlalu dan rahasianya tidak diputar.
8.3.5	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	secretsmanager-secret-periodic-rotation	Pastikan AWS rahasia Secrets Manager telah dirotasi dalam jumlah hari yang ditentukan sebelumnya. Aturannya adalah NON_COMPLIANT jika rahasia belum diputar selama lebih dari jumlah hari maxDaysSinceRotasi. Nilai defaultnya adalah 90 hari.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.7	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	access-keys-rotated	Pastikan kunci akses IAM aktif diputar (diubah) dalam jumlah hari yang ditentuka n dalam maxAccess Key Usia. Aturannya adalah NON_COMPL IANT jika kunci akses tidak diputar dalam jangka waktu yang ditentukan. Nilai defaultnya adalah 90 hari.
8.3.7	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	secretsmanager-sch eduled-rotation-su ccess-periksa	Pastikan AWS rahasia Secrets Manager diputar dengan sukses sesuai dengan jadwal rotasi. Secrets Manager menghitun g tanggal rotasi harus terjadi. Aturannya adalah NON_COMPL IANT jika tanggal berlalu dan rahasiany a tidak diputar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.7	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	secretsmanager-secret-periodic-rotation	Pastikan AWS rahasia Secrets Manager telah dirotasi dalam jumlah hari yang ditentukan sebelumnya. Aturannya adalah NON_COMPLIANT jika rahasia belum diputar selama lebih dari jumlah hari maxDaysSinceRotasi. Nilai defaultnya adalah 90 hari.
8.3.9	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	access-keys-rotated	Pastikan kunci akses IAM aktif diputar (diubah) dalam jumlah hari yang ditentukan dalam maxAccessKeyUsia. Aturannya adalah NON_COMPLIANT jika kunci akses tidak diputar dalam jangka waktu yang ditentukan. Nilai defaultnya adalah 90 hari.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.3.9	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	secretsmanager-scheduled-rotation-success-periksa	Pastikan AWS rahasia Secrets Manager diputar dengan sukses sesuai dengan jadwal rotasi. Secrets Manager menghitung tanggal rotasi harus terjadi. Aturannya adalah NON_COMPLIANT jika tanggal berlalu dan rahasianya tidak diputar.
8.3.9	Otentikasi yang kuat untuk pengguna dan administrator dibuat dan dikelola. (PCI-DSS-V4.0)	secretsmanager-secret-periodic-rotation	Pastikan AWS rahasia Secrets Manager telah dirotasi dalam jumlah hari yang ditentukan sebelumnya. Aturannya adalah NON_COMPLIANT jika rahasia belum diputar selama lebih dari jumlah hari maxDaysSinceRotasi. Nilai defaultnya adalah 90 hari.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.4.1	Otentikasi multi-faktor (MFA) diimplementasikan untuk mengamankan akses ke CDE. (PCI-DSS-V4.0)	s3- bucket-mfa-delete-enabled	Pastikan MFA Delete diaktifkan di konfigurasi pembuatan versi bucket Amazon Simple Storage Service (Amazon S3). Aturannya adalah NON_COMPLIANT jika MFA Delete tidak diaktifkan.
8.4.2	Otentikasi multi-faktor (MFA) diimplementasikan untuk mengamankan akses ke CDE. (PCI-DSS-V4.0)	s3- bucket-mfa-delete-enabled	Pastikan MFA Delete diaktifkan di konfigurasi pembuatan versi bucket Amazon Simple Storage Service (Amazon S3). Aturannya adalah NON_COMPLIANT jika MFA Delete tidak diaktifkan.
8.4.3	Otentikasi multi-faktor (MFA) diimplementasikan untuk mengamankan akses ke CDE. (PCI-DSS-V4.0)	s3- bucket-mfa-delete-enabled	Pastikan MFA Delete diaktifkan di konfigurasi pembuatan versi bucket Amazon Simple Storage Service (Amazon S3). Aturannya adalah NON_COMPLIANT jika MFA Delete tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.6.3	Penggunaan akun aplikasi dan sistem serta faktor otentikasi terkait dikelola dengan ketat. (PCI-DSS-V4.0)	access-keys-rotated	Pastikan kunci akses IAM aktif diputar (diubah) dalam jumlah hari yang ditentukan dalam maxAccessKeyUsia. Aturannya adalah NON_COMPLIANT jika kunci akses tidak diputar dalam jangka waktu yang ditentukan. Nilai defaultnya adalah 90 hari.
8.6.3	Penggunaan akun aplikasi dan sistem serta faktor otentikasi terkait dikelola dengan ketat. (PCI-DSS-V4.0)	secretsmanager-scheduled-rotation-success-periksa	Pastikan AWS rahasia Secrets Manager diputar dengan sukses sesuai dengan jadwal rotasi. Secrets Manager menghitung tanggal rotasi harus terjadi. Aturannya adalah NON_COMPLIANT jika tanggal berlalu dan rahasianya tidak diputar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.6.3	Penggunaan akun aplikasi dan sistem serta faktor otentikasi terkait dikelola dengan ketat. (PCI-DSS-V4.0)	secretsmanager-secret-periodic-rotation	Pastikan AWS rahasia Secrets Manager telah dirotasi dalam jumlah hari yang ditentukan sebelumnya. Aturannya adalah NON_COMPLIANT jika rahasia belum diputar selama lebih dari jumlah hari maxDaysSinceRotasi. Nilai defaultnya adalah 90 hari.
A1.1.2	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	neptune-cluster-snapshot-public-dilarang	Pastikan snapshot kluster DB manual Amazon Neptunus tidak bersifat publik. Aturannya adalah NON_COMPLIANT jika ada snapshot cluster Neptunus yang ada dan yang baru bersifat publik.
A1.1.2	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	docdb-cluster-snapshot-public-dilarang	Pastikan snapshot cluster manual Amazon DocumentDB tidak bersifat publik. Aturannya adalah NON_COMPLIANT jika ada snapshot cluster manual Amazon DocumentDB yang bersifat publik.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.1.2	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan brankas cadangan memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Aturannya adalah NON_COMPLIANT jika Brankas Cadangan tidak memiliki kebijakan berbasis sumber daya atau memiliki kebijakan tanpa pernyataan 'Deny' yang sesuai (pernyataan dengan cadangan: DeleteRecoveryPoint, cadangan:, dan cadangan: izin). UpdateRecoveryPointLifecycle PutBackupVaultAccessPolicy

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.1.2	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	emr-block-public-access	Pastikan akun dengan Amazon EMR telah mengaktifkan pengaturan akses publik yang memblokir. Aturannya adalah NON_COMPLIANT jika BlockPublicSecurityGroupRules salah, atau jika benar, port selain Port 22 terdaftar di. PermittedPublicSecurityGroupRuleRanges
A1.1.2	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	s3- -blok access-point-public-access	Pastikan jalur akses Amazon S3 telah mengaktifkan pengaturan akses publik blokir. Aturannya adalah NON_COMPLIANT jika pengaturan akses publik blok tidak diaktifkan untuk titik akses S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.1.2	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	s3- -blok account-level-public-access	Pastikan bahwa pengaturan blok akses publik yang diperlukan dikonfigurasi dari tingkat akun. Aturannya hanya NON_COMPLIANT jika bidang yang ditetapkan di bawah ini tidak cocok dengan bidang yang sesuai di item konfigurasi.
A1.1.2	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	s3- bucket-mfa-delete-enabled	Pastikan MFA Delete diaktifkan di konfigurasi pembuatan versi bucket Amazon Simple Storage Service (Amazon S3). Aturannya adalah NON_COMPLIANT jika MFA Delete tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	api-gw-endpoint-type-periksa	Pastikan bahwa Amazon API Gateway APIs adalah tipe yang ditentukan dalam parameter aturan 'endpointConfigurationType'. Aturan mengembalikan NON_COMPLIANT jika REST API tidak cocok dengan tipe titik akhir yang dikonfigurasi dalam parameter aturan.
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	cloudfront-associated-with-waf	Pastikan CloudFront distribusi Amazon dikaitkan dengan firewall aplikasi web (WAF) atau daftar kontrol akses WAFv2 web (ACLs). Aturannya adalah NON_COMPLIANT jika CloudFront distribusi tidak terkait dengan ACL web WAF.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	cloudfront-custom-ssl-certificate	Pastikan sertifikat yang terkait dengan CloudFront distribusi Amazon bukan sertifikat SSL default. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi menggunakan sertifikat SSL default.
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	netfw-policy-default-action-fragmen-paket	Pastikan kebijakan AWS Network Firewall dikonfigurasi dengan tindakan default stateless yang ditentukan pengguna untuk paket terfragmentasi. Aturannya adalah NON_COMPLIANT jika tindakan default stateless untuk paket terfragmentasi tidak cocok dengan tindakan default yang ditentukan pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	rds-db-security-group-tidak diizinkan	Pastikan bahwa grup keamanan Amazon Relational Database Service (Amazon RDS) DB adalah yang default. Aturannya adalah NON_COMPLIANT jika ada grup keamanan DB yang bukan grup keamanan DB default.
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan	Pastikan Gateway Transit Amazon Elastic Compute Cloud (Amazon EC2) tidak mengaktifkan "AutoAcceptSharedAttachments. Aturannya adalah NON_COMPLIANT untuk Transit Gateway jika " disetel ke AutoAcceptSharedAttachments 'aktifkan'.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	eks-endpoint-no-public-akses	Pastikan titik akhir Amazon Elastic Kubernetes Service (Amazon EKS) tidak dapat diakses publik. Aturannya adalah NON_COMPLIANT jika titik akhir dapat diakses publik.
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	terbatas-ssh	Catatan: Untuk aturan ini, pengidentifikasi aturan (INCOMING_SSH_DISABLED) dan nama aturan (restricted-ssh) berbeda. Pastikan bahwa lalu lintas SSH yang masuk untuk grup keamanan dapat diakses. Aturannya adalah COMPLIANT jika alamat IP dari lalu lintas SSH yang masuk dalam grup keamanan dibatasi (CIDR selain 0.0.0.0/0 atau: :/0). Jika tidak, NON_COMPLIANT.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	appsync-associated-with-waf	Pastikan AWS AppSync APIs yang terkait dengan daftar kontrol akses AWS WAFv2 web (ACLs). Aturannya adalah NON_COMPLIANT untuk AWS AppSync API jika tidak terkait dengan ACL web.
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	docdb-cluster-snapshot-public-dilarang	Pastikan snapshot cluster manual Amazon DocumentDB tidak bersifat publik. Aturannya adalah NON_COMPLIANT jika ada snapshot cluster manual Amazon DocumentDB yang bersifat publik.
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	codebuild-project-source-repo-url-periksa	Pastikan URL repositori sumber Bitbucket TIDAK berisi kredensyal masuk atau tidak. Aturannya adalah NON_COMPLIANT jika URL berisi informasi login dan COMPLIANT jika tidak.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	elb-acm-certificate-required	Pastikan Classic Load Balancers menggunakan sertifikat SSL yang disediakan oleh Certificate Manager AWS . Untuk menggunakan aturan ini, gunakan pendengar SSL atau HTTPS dengan Classic Load Balancer Anda. Catatan - aturan ini hanya berlaku untuk Classic Load Balancers . Aturan ini tidak memeriksa Application Load Balancers dan Network Load Balancers.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	emr-block-public-access	Pastikan akun dengan Amazon EMR telah mengaktifkan pengaturan akses publik yang memblokir. Aturannya adalah NON_COMPLIANT jika BlockPublicSecurityGroupRules salah, atau jika benar, port selain Port 22 terdaftar di. PermittedPublicSecurityGroupRuleRanges
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	nacl-no-unrestricted-ssh-rdp	Pastikan port default untuk lalu lintas masuk SSH/RDP untuk daftar kontrol akses jaringan () dibatasi. NACLs Aturannya adalah NON_COMPLIANT jika entri masuk NACL memungkinkan blok sumber TCP atau UDP CIDR untuk port 22 atau 3389.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	waf-global-webacl-not-kosong	Pastikan bahwa WAF Global Web ACL berisi beberapa aturan WAF atau grup aturan. Aturan ini adalah NON_COMPLIANT jika ACL Web tidak berisi aturan WAF atau grup aturan.
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	waf-global-rulegroup-not-kosong	Pastikan grup aturan AWS WAF Classic berisi beberapa aturan. Aturannya adalah NON_COMPLIANT jika tidak ada aturan yang ada dalam grup aturan.
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	waf-global-rule-not-kosong	Pastikan bahwa aturan global AWS WAF berisi beberapa kondisi. Aturannya adalah NON_COMPLIANT jika tidak ada kondisi dalam aturan global WAF.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	ec2- -semua client-vpn-not-authorize	Pastikan bahwa aturan otorisasi AWS Client VPN tidak mengotorisasi akses koneksi untuk semua klien. Aturannya adalah NON_COMPLIANT jika 'AccessAll' hadir dan disetel ke true.
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	internet-gateway-authorized-vpc-hanya	Pastikan gateway internet dilampirkan ke cloud pribadi virtual resmi (Amazon VPC). Aturannya adalah NON_COMPLIANT jika gateway internet dilampirkan ke VPC yang tidak sah.
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	s3- -blok access-point-public-access	Pastikan jalur akses Amazon S3 telah mengaktifkan pengaturan akses publik blokir. Aturannya adalah NON_COMPLIANT jika pengaturan akses publik blok tidak diaktifkan untuk titik akses S3.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.1.3	Penyedia layanan multi-tenant melindungi dan memisahkan semua lingkungan dan data pelanggan. (PCI-DSS-V4.0)	s3- -blok account-level-public-access	Pastikan bahwa pengaturan blok akses publik yang diperlukan dikonfigurasi dari tingkat akun. Aturannya hanya NON_COMPLIANT jika bidang yang ditetapkan di bawah ini tidak cocok dengan bidang yang sesuai di item konfigurasi.
A1.2.1	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	api-gwv2- access-logs-enabled	Pastikan bahwa tahap Amazon API Gateway V2 mengaktifkan pencatatan akses. Aturannya adalah NON_COMPLIANT jika 'accessLogSettings' tidak ada dalam konfigurasi Stage.
A1.2.1	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.2.1	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	cloudfront-accesslogs-enabled	Pastikan CloudFront distribusi Amazon dikonfigurasi untuk mengirimkan log akses ke bucket Amazon S3. Aturannya adalah NON_COMPLIANT jika CloudFront distribusi tidak memiliki logging yang dikonfigurasi.
A1.2.1	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	cloudtrail-security-trail-enabled	Pastikan bahwa setidaknya ada satu AWS CloudTrail jejak yang ditentukan dengan praktik terbaik keamanan. Aturan ini SESUAI jika setidaknya ada satu jejak yang memenuhi semua hal berikut:
A1.2.1	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	neptune-cluster-cloudwatch-log-ekspor diaktifkan	Pastikan klaster CloudWatch Amazon Neptunus mengaktifkan ekspor log untuk log audit. Aturannya adalah NON_COMPLIANT jika cluster Neptunus tidak mengaktifkan ekspor log untuk log audit. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.2.1	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	ecs-task-definition-log-konfigurasi	Pastikan bahwa LogConfiguration diatur pada Definisi Tugas ECS aktif. Aturan ini NON_COMPLIANT jika ECSTask Definisi aktif tidak memiliki sumber daya LogConfiguration yang ditentukan atau nilai untuk LogConfiguration adalah null dalam setidaknya satu definisi kontainer.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.2.1	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	cloudtrail-diaktifkan	Catatan: Untuk aturan ini, pengidentifikasi aturan (CLOUD_TRAIL_ENABLED) dan nama aturan (cloudtrail-enabled) berbeda. Pastikan AWS CloudTrail jejak diaktifkan di AWS akun Anda. Aturannya adalah NON_COMPLIANT jika jejak tidak diaktifkan. Secara opsional, aturan memeriksa bucket S3 tertentu, topik Amazon Simple Notification Service (Amazon SNS), dan grup log. CloudWatch

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.2.1	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	multi-region-cloudtrail-enabled	Catatan: untuk aturan ini, pengidentifikasi aturan (MULTI_REGION_CLOUD_TRAIL_ENABLED) dan nama aturan () berbeda. multi-region-cloudtrail-enabled Pastikan setidaknya ada satu multi-wilayah AWS CloudTrail. Aturannya adalah NON_COMPLIANT jika jejak tidak cocok dengan parameter input. Aturannya adalah NON_COMPLIANT jika ExcludeManagementEventSources bidang tidak kosong atau jika AWS CloudTrail dikonfigurasi untuk mengecualikan peristiwa manajemen seperti peristiwa AWS KMS atau peristiwa API Data Amazon RDS.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.2.1	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	appsync-logging-enabled	Pastikan bahwa AWS AppSync API telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika logging tidak diaktifkan, atau 'fieldLogLevel' bukan ERROR atau SEMUA.
A1.2.1	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	waf-classic-logging-enabled	Pastikan pencatatan diaktifkan pada daftar kontrol akses web global klasik AWS WAF (web ACLs). Aturannya adalah NON_COMPLIANT untuk ACL web global, jika tidak mengaktifkan logging.
A1.2.1	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	mq-cloudwatch-audit-logging-diaktifkan	Pastikan pialang Amazon MQ mengaktifkan pencatatan CloudWatch audit Amazon. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.2.1	Penyedia layanan multi-tenant memfasili tasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	mq-cloudwatch-audit-log-diaktifkan	Pastikan bahwa broker Amazon MQ mengaktif kan pencatatan CloudWatch audit. Aturannya adalah NON_COMPLIANT jika broker tidak mengaktifkan audit logging.
A1.2.1	Penyedia layanan multi-tenant memfasili tasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	eks-cluster-logging-enabled	Pastikan klaster Amazon Elastic Kubernetes Service (Amazon EKS) dikonfigurasi dengan logging diaktifkan. Aturannya adalah NON_COMPLIANT jika logging untuk klaster Amazon EKS tidak diaktifkan untuk semua jenis log.
A1.2.1	Penyedia layanan multi-tenant memfasili tasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	elastic-beanstalk-logs-to-jam tangan awan	Pastikan lingkunga n AWS Elastic Beanstalk dikonfigu rasi untuk mengirim log ke Amazon Logs. CloudWatch Aturannya adalah NON_COMPLIANT jika nilai `StreamLogs` salah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.2.1	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	step-functions-state-machine-logging-diaktifkan	Pastikan bahwa mesin AWS Step Functions telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika mesin status tidak mengaktifkan logging atau konfigurasi logging tidak pada tingkat minimum yang disediakan.
A1.2.1	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	netfw-logging-enabled	Pastikan firewall AWS Network Firewall telah mengaktifkan logging. Aturannya adalah NON_COMPLIANT jika jenis logging tidak dikonfigurasi. Anda dapat menentukan jenis logging yang Anda ingin aturan untuk memeriksa.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A1.2.3	Penyedia layanan multi-tenant memfasilitasi pencatatan dan respons insiden untuk semua pelanggan. (PCI-DSS-V4.0)	security-account-information-provided	Pastikan bahwa Anda telah memberikan informasi kontak keamanan untuk kontak AWS akun Anda. Aturannya adalah NON_COMPLIANT jika informasi kontak keamanan dalam akun tidak disediakan.
A3.2.5.1	Cakupan PCI DSS didokumentasikan dan divalidasi. (PCI-DSS-V4.0)	macie-auto-sensitive-data-penemuan-cek	Pastikan penemuan data sensitif otomatis diaktifkan untuk Amazon Macie. Aturannya adalah NON_COMPLIANT jika penemuan data sensitif otomatis dinonaktifkan. Aturan ini BERLAKU untuk akun administrator dan NOT_APPLICABLE untuk akun anggota.
A3.2.5.1	Cakupan PCI DSS didokumentasikan dan divalidasi. (PCI-DSS-V4.0)	macie-status-check	Pastikan Amazon Macie diaktifkan di akun Anda per wilayah. Aturannya adalah NON_COMPLIANT jika atribut 'status' tidak disetel ke 'ENABLED'.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.2.5.2	Cakupan PCI DSS didokumentasikan dan divalidasi. (PCI-DSS-V4.0)	macie-auto-sensitive-data-penemuan-cek	Pastikan penemuan data sensitif otomatis diaktifkan untuk Amazon Macie. Aturannya adalah NON_COMPLIANT jika penemuan data sensitif otomatis dinonaktifkan. Aturan ini BERLAKU untuk akun administrator dan NOT_APPLI CABLE untuk akun anggota.
A3.2.5.2	Cakupan PCI DSS didokumentasikan dan divalidasi. (PCI-DSS-V4.0)	macie-status-check	Pastikan Amazon Macie diaktifkan di akun Anda per wilayah. Aturannya adalah NON_COMPL IANT jika atribut 'status' tidak disetel ke 'ENABLED'.
A3.3.1	PCI DSS dimasukka n ke dalam kegiatan business-as-usual (BAU). (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifka n di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.3.1	PCI DSS dimasukkan ke dalam kegiatan business-as-usual (BAU). (PCI-DSS-V4.0)	cloudformation-stack-notification-check	Pastikan CloudFormation tumpukan Anda mengirim pemberitahuan acara ke topik Amazon SNS. Secara opsional pastikan bahwa topik Amazon SNS yang ditentukan digunakan. Aturannya adalah NON_COMPLIANT jika CloudFormation tumpukan tidak mengirim notifikasi.
A3.3.1	PCI DSS dimasukkan ke dalam kegiatan business-as-usual (BAU). (PCI-DSS-V4.0)	ec2- instance-detailed-monitoring-enabled	Pastikan pemantauan terperinci diaktifkan untuk EC2 instans. Aturannya adalah NON_COMPLIANT jika pemantauan terperinci tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.3.1	PCI DSS dimasukkan ke dalam kegiatan business-as-usual (BAU). (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.3.1	PCI DSS dimasukkan ke dalam kegiatan business-as-usual (BAU). (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.3.1	PCI DSS dimasukkan ke dalam kegiatan business-as-usual (BAU). (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.3.1	PCI DSS dimasukkan ke dalam kegiatan business-as-usual (BAU). (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.3.1	PCI DSS dimasukkan ke dalam kegiatan business-as-usual (BAU). (PCI-DSS-V4.0)	cloudwatch-alarm-resource-check	Pastikan bahwa jenis sumber daya memiliki CloudWatch alarm untuk metrik bernama. Untuk jenis sumber daya, Anda dapat menentukan volume EBS, EC2 instans, kluster Amazon RDS, atau bucket S3. Aturannya adalah COMPLIANT jika metrik bernama memiliki ID sumber daya dan CloudWatch alarm.
A3.3.1	PCI DSS dimasukkan ke dalam kegiatan business-as-usual (BAU). (PCI-DSS-V4.0)	cloudwatch-alarm-settings-check	Pastikan CloudWatch alarm dengan nama metrik yang diberikan memiliki pengaturan yang ditentukan.
A3.3.1	PCI DSS dimasukkan ke dalam kegiatan business-as-usual (BAU). (PCI-DSS-V4.0)	wafv2- rulegroup-logging-enabled	Pastikan pengumpulan metrik CloudWatch keamanan Amazon pada grup AWS WAFv2 aturan diaktifkan. Aturannya adalah NON_COMPLIANT jika '. VisibilityConfig CloudWatchMetricsEnabled'bidang disetel ke false.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.3.1	PCI DSS dimasukkan ke dalam kegiatan business-as-usual (BAU). (PCI-DSS-V4.0)	sns-topic-message-delivery-notifikasi-diaktifkan	Pastikan pencatatan Amazon Simple Notification Service (SNS) diaktifkan untuk status pengiriman pesan notifikasi yang dikirim ke topik untuk titik akhir. Aturannya adalah NON_COMPLIANT jika pemberitahuan status pengiriman untuk pesan tidak diaktifkan.
A3.4.1	Akses logis ke lingkungan data pemegang kartu dikendalikan dan dikelola. (PCI-DSS-V4.0)	neptune-cluster-snapshot-public-dilarang	Pastikan snapshot kluster DB manual Amazon Neptunus tidak bersifat publik. Aturannya adalah NON_COMPLIANT jika ada snapshot cluster Neptunus yang ada dan yang baru bersifat publik.
A3.4.1	Akses logis ke lingkungan data pemegang kartu dikendalikan dan dikelola. (PCI-DSS-V4.0)	docdb-cluster-snapshot-public-dilarang	Pastikan snapshot cluster manual Amazon DocumentDB tidak bersifat publik. Aturannya adalah NON_COMPLIANT jika ada snapshot cluster manual Amazon DocumentDB yang bersifat publik.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.4.1	Akses logis ke lingkungan data pemegang kartu dikendalikan dan dikelola. (PCI-DSS-V4.0)	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan brankas cadangan memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan. Aturannya adalah NON_COMPLIANT jika Brankas Cadangan tidak memiliki kebijakan berbasis sumber daya atau memiliki kebijakan tanpa pernyataan 'Deny' yang sesuai (pernyataan dengan cadangan: DeleteRecoveryPoint, cadangan:, dan cadangan: izin). UpdateRecoveryPointLifecycle PutBackupVaultAccessPolicy

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.4.1	Akses logis ke lingkungan data pemegang kartu dikendalikan dan dikelola. (PCI-DSS-V4.0)	emr-block-public-access	Pastikan akun dengan Amazon EMR telah mengaktifkan pengaturan akses publik yang memblokir. Aturannya adalah NON_COMPLIANT jika BlockPublicSecurityGroupRules salah, atau jika benar, port selain Port 22 terdaftar di. PermittedPublicSecurityGroupRuleRanges
A3.4.1	Akses logis ke lingkungan data pemegang kartu dikendalikan dan dikelola. (PCI-DSS-V4.0)	secretsmanager-secret-unused	Pastikan AWS rahasia Secrets Manager telah diakses dalam beberapa hari tertentu. Aturannya adalah NON_COMPLIANT jika rahasia belum diakses dalam jumlah hari unusedForDays ". Nilai defaultnya adalah 90 hari.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.4.1	Akses logis ke lingkungan data pemegang kartu dikendalikan dan dikelola. (PCI-DSS-V4.0)	s3- -blok access-point-public-access	Pastikan jalur akses Amazon S3 telah mengaktif kan pengaturan akses publik blokir. Aturannya adalah NON_COMPLIANT jika pengaturan akses publik blok tidak diaktifkan untuk titik akses S3.
A3.4.1	Akses logis ke lingkungan data pemegang kartu dikendalikan dan dikelola. (PCI-DSS-V4.0)	s3- -blok account-level-public-access	Pastikan bahwa pengaturan blok akses publik yang diperlukan dikonfigu rasi dari tingkat akun. Aturannya hanya NON_COMPLIANT jika bidang yang ditetapkan di bawah ini tidak cocok dengan bidang yang sesuai di item konfigurasi.
A3.4.1	Akses logis ke lingkungan data pemegang kartu dikendalikan dan dikelola. (PCI-DSS-V4.0)	s3- bucket-mfa-delete-enabled	Pastikan MFA Delete diaktifkan di konfigura si pembuatan versi bucket Amazon Simple Storage Service (Amazon S3). Aturannya adalah NON_COMPLIANT jika MFA Delete tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.5.1	Peristiwa mencurigakan diidentifikasi dan ditanggapi. (PCI-DSS-V4.0)	api-gw-xray-enabled	Pastikan penelusuran AWS X-Ray diaktifkan di Amazon API Gateway REST APIs. Aturannya SESUAI jika penelusuran X-Ray diaktifkan dan NON_COMPLIANT sebaliknya.
A3.5.1	Peristiwa mencurigakan diidentifikasi dan ditanggapi. (PCI-DSS-V4.0)	cloudformation-stack-notification-check	Pastikan CloudFormation tumpukan Anda mengirim pemberitahuan acara ke topik Amazon SNS. Secara opsional pastikan bahwa topik Amazon SNS yang ditentukan digunakan. Aturannya adalah NON_COMPLIANT jika CloudFormation tumpukan tidak mengirim notifikasi.
A3.5.1	Peristiwa mencurigakan diidentifikasi dan ditanggapi. (PCI-DSS-V4.0)	ec2- instance-detailed-monitoring-enabled	Pastikan pemantauan terperinci diaktifkan untuk EC2 instans. Aturannya adalah NON_COMPLIANT jika pemantauan terperinci tidak diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.5.1	Peristiwa mencurigakan diidentifikasi dan ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.5.1	Peristiwa mencurigakan diidentifikasi dan ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.5.1	Peristiwa mencurigakan diidentifikasi dan ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.5.1	Peristiwa mencurigakan diidentifikasi dan ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-action-check	Pastikan CloudWatch alarm memiliki tindakan yang dikonfigurasi untuk status ALARM, INSUFFICIENT_DATA, atau OK. Secara opsional memastikan bahwa tindakan apa pun cocok dengan ARN bernama. Aturannya adalah NON_COMPLIANT jika tidak ada tindakan yang ditentukan untuk alarm atau parameter opsional.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.5.1	Peristiwa mencurigakan diidentifikasi dan ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-resource-check	Pastikan bahwa jenis sumber daya memiliki CloudWatch alarm untuk metrik bernama. Untuk jenis sumber daya, Anda dapat menentukan volume EBS, EC2 instans, kluster Amazon RDS, atau bucket S3. Aturannya adalah COMPLIANT jika metrik bernama memiliki ID sumber daya dan CloudWatch alarm.
A3.5.1	Peristiwa mencurigakan diidentifikasi dan ditanggapi. (PCI-DSS-V4.0)	cloudwatch-alarm-settings-check	Pastikan CloudWatch alarm dengan nama metrik yang diberikan memiliki pengaturan yang ditentukan.
A3.5.1	Peristiwa mencurigakan diidentifikasi dan ditanggapi. (PCI-DSS-V4.0)	wafv2- rulegroup-logging-enabled	Pastikan pengumpulan metrik CloudWatch keamanan Amazon pada grup AWS WAFv2 aturan diaktifkan. Aturannya adalah NON_COMPLIANT jika '. VisibilityConfig CloudWatchMetricsEnabled'bidang disetel ke false.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
A3.5.1	Peristiwa mencurigakan diidentifikasi dan ditanggapi. (PCI-DSS-V4.0)	sns-topic-message-delivery-notifikasi-diaktifkan	Pastikan pencatatan Amazon Simple Notification Service (SNS) diaktifkan untuk status pengiriman pesan notifikasi yang dikirim ke topik untuk titik akhir. Aturannya adalah NON_COMPLIANT jika pemberitahuan status pengiriman untuk pesan tidak diaktifkan.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk PCI DSS 4.0 (Termasuk jenis sumber daya global).

Praktik Terbaik Operasional untuk Sumber Daya yang Dapat Diakses Publik

Paket kesesuaian ini membantu mengidentifikasi sumber daya yang mungkin dapat diakses publik.

Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Sumber Daya yang Dapat Diakses Publik.

Praktik Terbaik Operasional untuk Kerangka Keamanan Cyber RBI untuk UCBs

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara Kerangka Keamanan Siber Reserve Bank of India (RBI) untuk Urban Cooperative Banks (UCBs) dan aturan AWS Config yang dikelola. Setiap aturan Config berlaku untuk AWS sumber daya tertentu, dan terkait dengan satu atau beberapa RBI Cyber Security Framework untuk kontrol. UCBs Kerangka Keamanan Cyber RBI untuk UCBs kontrol dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (1.1)	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (1.1)	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizat ions membantu memastika n bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabk an konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.
Lampiran_I (1.1)	ecr-private-tag-immutability-diaktifkan	Aktifkan Kekekalan Tag Elastic Container Repositor y (ECR) untuk mencegah tag gambar pada gambar ECR Anda ditimpa. Sebelumny a, tag dapat ditimpa yang membutuhkan metodologi manual untuk mengidentifikasi gambar secara unik.
Lampiran_I (1.3)	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastika n sertifikat X509 dikeluark an oleh AWS ACM. Sertifika t ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (1.3)	alb-http-drop-invalid-Header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Lampiran_I (1.3)	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalanan, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihkan permintaan HTTP yang tidak terenkripsi ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Lampiran_I (1.3)	api-gw-cache-enabled-dan-dienkripsi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk cache tahap API Gateway Anda. Karena data sensitif dapat ditangkap untuk metode API, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (1.3)	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.
Lampiran_I (1.3)	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifika t SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.
Lampiran_I (1.3)	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan membantu melindung i data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (1.3)	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Lampiran_I (1.3)	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
Lampiran_I (1.3)	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.
Lampiran_I (1.3)	backup-recovery-point-encrypted	Pastikan enkripsi diaktifkan untuk titik pemulihan AWS Backup Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Lampiran_I (1.3)	codebuild-project-artifact-encryption	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk AWS CodeBuild artefak Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (1.3)	codebuild-project-s3-log-terenkripsi	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk AWS CodeBuild log Anda yang disimpan di Amazon S3.
Lampiran_I (1.3)	opensearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon Anda.
Lampiran_I (1.3)	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
Lampiran_I (1.3)	opensearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifkan. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikasi dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (1.3)	dynamodb-table-encrypted-kms	Pastikan enkripsi diaktifkan untuk tabel Amazon DynamoDB Anda. Karena data sensitif dapat ada saat diam di tabel ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut. Secara default, tabel DynamoDB dienkripsi dengan kunci master pelanggan (CMK) AWS yang dimiliki.
Lampiran_I (1.3)	ec2- ebs-encryption-by-default	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Lampiran_I (1.3)	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (1.3)	elasticsearch-encrypted-at-rest	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk domain OpenSearch Layanan Amazon (OpenSearch Layanan) Anda.
Lampiran_I (1.3)	elasticsearch-node-to-node-pemeriksaan enkripsi-	Pastikan node-to-node enkripsi untuk OpenSearch Layanan Amazon diaktifka n. Node-to-nodeenkripsi memungkinkan enkripsi TLS 1.2 untuk semua komunikas i dalam Amazon Virtual Private Cloud (Amazon VPC). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Lampiran_I (1.3)	elb-acm-certificate-required	Karena data sensitif dapat ada dan membantu melindung i data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebark an sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (1.3)	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Lampiran_I (1.3)	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
Lampiran_I (1.3)	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindung i data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperluka n pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (1.3)	rds-snapshot-encrypted	Pastikan enkripsi diaktifkan untuk snapshot Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat istirahat, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Lampiran_I (1.3)	rds-storage-encrypted	Untuk membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk instans Amazon Relational Database Service (Amazon RDS) Anda. Karena data sensitif dapat ada saat diam di instans Amazon RDS, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (1.3)	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
Lampiran_I (1.3)	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (1.3)	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
Lampiran_I (1.3)	s3- bucket-ssl-requests-only	Untuk membantu melindung i data dalam perjalanan, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerluka n permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
Lampiran_I (1.3)	sagemaker-endpoint-configur ation-kms-kunci-dikonfigurasi	Untuk membantu melindung i data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk titik SageMaker akhir Anda. Karena data sensitif dapat ada saat istirahat di SageMaker titik akhir, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (1.3)	sagemaker-notebook-instance-kms-kunci-dikonfigurasi	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk SageMaker notebook Anda. Karena data sensitif dapat ada saat diam di SageMaker notebook, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Lampiran_I (1.3)	sns-encrypted-kms	Untuk membantu melindungi data saat istirahat, pastikan topik Amazon Simple Notification Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
Lampiran_I (1.3)	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (1.3)	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
Lampiran_I (1.3)	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
Lampiran_I (1.3)	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (1.3)	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses secara publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
Lampiran_I (1.3)	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (1.3)	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
Lampiran_I (1.3)	no-unrestricted-route-to-igw	Pastikan tabel EC2 rute Amazon tidak memiliki rute tak terbatas ke gateway internet. Menghapus atau membatasi akses ke internet untuk beban kerja di Amazon VPCs dapat mengurangi akses yang tidak diinginkan di lingkungan Anda.
Lampiran_I (1.3)	redshift-cluster-kms-enabled	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk klaster Amazon Redshift Anda. Karena data sensitif dapat ada saat diam di cluster Redshift, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (1.3)	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspo s informasi tentang akun, sumber daya, dan proses internal Anda.
Lampiran_I (1.3)	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (1.3)	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkin kan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabk an akses tidak sah ke sumber daya VPC Amazon.
Lampiran_I (1.3)	lambda-function-public-acce ss-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (1.3)	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyarat an untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.
Lampiran_I (1.3)	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (1.3)	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.
Lampiran_I (1.3)	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (1.3)	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,338 9,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
Lampiran_I (1.3)	s3- -dilarang bucket-level-publi c-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (1.3)	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
Lampiran_I (1.3)	s3- bucket-public-read-prohibit ed	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (1.3)	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
Lampiran_I (1.3)	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (5.1)	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploitasi web umum. Eksploitasi web ini dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.
Lampiran_I (5.1)	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelolaan akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .
Lampiran_I (5.1)	waf-regional-rule-not-kosong	Pastikan AWS WAF Anda memiliki aturan yang tidak kosong. Aturan tanpa kondisi dapat mengakibatkan perilaku yang tidak diinginkan.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (5.1)	waf-regional-rulegroup-not-kosong	Pastikan AWS WAF Anda memiliki grup aturan yang tidak kosong. Grup aturan yang kosong dapat mengakibatkan perilaku yang tidak diinginkan.
Lampiran_I (5.1)	waf-regional-webacl-not-kosong	Web ACL yang dilampirkan ke AWS WAF dapat berisi kumpulan aturan dan kelompok aturan untuk memeriksa dan mengontrol permintaan web. Jika ACL Web kosong, lalu lintas web lewat tanpa terdeteksi atau ditindaklanjuti oleh WAF.
Lampiran_I (5.1)	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (5.1)	api-gw-associated-with-waf	AWS WAF memungkin kan Anda mengonfigurasi seperangkat aturan (disebut daftar kontrol akses web (web ACL)) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan tahap Amazon API Gateway Anda dikaitkan dengan WAF Web ACL untuk melindung inya dari serangan berbahaya
Lampiran_I (5.1)	dibatasi ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (5.1)	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,338 9,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
Lampiran_I (6)	ec2- -periksa managedin stance-association-complian ce-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapka n status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigura si aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (6)	ec2- -periksa managedin stance-patch-compliance-sta tus	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
Lampiran_I (6)	guardduty-non-archived-find ings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan: rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighS ev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (6)	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.
Lampiran_I (6)	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relational Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (6)	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00 -sat: 16:30), dan automated SnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
Lampiran_I (6)	vuln-management-plan-exists (pemeriksaan proses)	Pastikan rencana manajemen kerentanan dikembangkan dan diimplementasikan untuk memiliki proses yang ditentukan secara formal untuk mengatasi kerentanan di lingkungan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (7.1)	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
Lampiran_I (7.1)	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (7.1)	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.
Lampiran_I (7.1)	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurang i peluang bagi identitas untuk menerima atau mempertah ankan hak istimewa yang berlebihan.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (7.1)	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (7.2)	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
Lampiran_I (7.3)	dibatasi ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.
Lampiran_I (7.4)	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.
Lampiran_I (7.4)	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (7.4)	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penol akan dengan merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilka n, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
Lampiran_I (7.4)	cloudtrail-s3-dataevents-di aktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.
Lampiran_I (7.4)	elasticsearch-logs-to-cloud watch	Pastikan domain OpenSearc h Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersediaan.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (7.4)	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS
Lampiran_I (7.4)	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (7.4)	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatatan ELB diaktifka n. Data yang dikumpulkan memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.
Lampiran_I (7.4)	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (7.4)	opensearch-audit-logging-enabled	Pastikan pencatatan audit diaktifkan di domain OpenSearch Layanan Amazon Anda. Pencatatan audit memungkinkan Anda melacak aktivitas pengguna di OpenSearch domain Anda, termasuk keberhasilan dan kegagalan otentikasi, permintaan, perubahan indeks OpenSearch, dan kueri penelusuran yang masuk.
Lampiran_I (7.4)	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearch Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.
Lampiran_I (7.4)	redshift-audit-logging-enabled	Untuk menangkap informasi tentang koneksi dan aktivitas pengguna di klaster Amazon Redshift, pastikan pencatatan audit diaktifkan.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (7.4)	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimk an file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REGION_CLOUD _TRAIL_ENABLED diaktifka n. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (7.4)	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.
Lampiran_I (7.4)	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (7.4)	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
Lampiran_I (7.4)	wafv2-logging diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (7.4)	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
Lampiran_I (10.2)	security-awareness-program-exists (pemeriksaan proses)	Membangun dan memeliharaa program kesadaran keamanan untuk organisasi Anda. Program kesadaran keamanan mendidik karyawan tentang cara melindungi organisasi mereka dari berbagai pelanggaran atau insiden keamanan.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (12)	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.
Lampiran_I (12)	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (12)	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadang an berkelanjutan dari tabel Anda selama 35 hari terakhir.
Lampiran_I (12)	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (12)	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
Lampiran_I (12)	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (12)	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (12)	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadangan otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.
Lampiran_I (12)	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk klaster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (12)	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relational Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.
Lampiran_I (12)	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersedi aan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersediaan data tetap terjaga.

ID Kontrol	AWS Aturan Config	Bimbingan
Lampiran_I (12)	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihka n setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Kerangka Keamanan Cyber RBI untuk UCBs.

Praktik Terbaik Operasional untuk RBI MD-ITF

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini memberikan contoh pemetaan antara Master Direction Reserve Bank of India (RBI) - Kerangka Teknologi Informasi dan aturan AWS Config yang dikelola. Setiap aturan Config berlaku

untuk AWS sumber daya tertentu, dan berhubungan dengan satu atau lebih RBI Master Direction - kontrol Kerangka Teknologi Informasi. Arah Master RBI - Kontrol Kerangka Teknologi Informasi dapat dikaitkan dengan beberapa aturan Config. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (a)	Identifikasi dan Klasifikasi Aset Informasi.	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.
3.1 (a)	Identifikasi dan Klasifikasi Aset Informasi.	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan, sesuai dengan standar organisasi Anda.
3.1 (a)	Identifikasi dan Klasifikasi Aset Informasi.	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (a)	Identifikasi dan Klasifikasi Aset Informasi.	ecr-private-tag-immutability-diaktifkan	Aktifkan Kekekalan Tag Elastic Container Repository (ECR) untuk mencegah tag gambar pada gambar ECR Anda ditimpa. Sebelumnya, tag dapat ditimpa yang membutuhkan metodologi manual untuk mengidentifikasi gambar secara unik.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (c)	Kontrol Akses Berbasis Peran	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (c)	Kontrol Akses Berbasis Peran	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (c)	Kontrol Akses Berbasis Peran	ecs-task-definition-nonroot-pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan bahwa pengguna non-root ditunjuk untuk mengakses definisi tugas Amazon Elastic Container Service (Amazon ECS) Anda.
3.1 (c)	Kontrol Akses Berbasis Peran	efs-access-point-enforce-root-direktori	Menegakkan direktori root untuk jalur akses Amazon Elastic File System (Amazon EFS) membantu membatasi akses data dengan memastikan bahwa pengguna jalur akses hanya dapat menjangkau file dari subdirektori yang ditentukan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (c)	Kontrol Akses Berbasis Peran	efs-access-point-enforce-identitas pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan penegakan pengguna diaktifkan untuk Amazon Elastic File System (Amazon EFS) Anda. Saat diaktifkan, Amazon EFS mengganti kan pengguna dan grup klien NFS IDs dengan identitas yang dikonfigurasi pada titik akses untuk semua operasi sistem file dan hanya memberika n akses ke identitas pengguna yang diberlakukan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (c)	Kontrol Akses Berbasis Peran	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (c)	Kontrol Akses Berbasis Peran	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (c)	Kontrol Akses Berbasis Peran	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (c)	Kontrol Akses Berbasis Peran	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (c)	Kontrol Akses Berbasis Peran	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (c)	Kontrol Akses Berbasis Peran	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (c)	Kontrol Akses Berbasis Peran	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredensyal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (c)	Kontrol Akses Berbasis Peran	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (c)	Kontrol Akses Berbasis Peran	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsageUsia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (c)	Kontrol Akses Berbasis Peran	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.
3.1 (c)	Kontrol Akses Berbasis Peran	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (c)	Kontrol Akses Berbasis Peran	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredensyal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (c)	Kontrol Akses Berbasis Peran	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensyal masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (c)	Kontrol Akses Berbasis Peran	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensyal masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
3.1 (c)	Kontrol Akses Berbasis Peran	secretsmanager-rotation-enabled-check	Aturan ini memastikan AWS rahasia Secrets Manager telah diaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (c)	Kontrol Akses Berbasis Peran	secretsmanager-scheduled-rotation-success-periksa	Aturan ini memastikan bahwa AWS rahasia Secrets Manager telah berhasil diputar sesuai dengan jadwal rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode di mana rahasia aktif, dan berpotensi mengurangi dampak bisnis jika dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (g)	Manajemen Insiden	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (g)	Manajemen Insiden	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (g)	Manajemen Insiden	alb-waf-enabled	Pastikan AWS WAF diaktifkan pada Elastic Load Balancers (ELB) untuk membantu melindungi aplikasi web. WAF membantu melindungi aplikasi web Anda atau APIs terhadap eksploita si web umum. Eksploitasi web ini dapat memengaru hi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan di lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (g)	Manajemen Insiden	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (g)	Manajemen Insiden	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
3.1 (h)	Jejak	api-gw-execution-logging-diaktifkan	Pencatatan API Gateway menampilkan tampilan mendetail dari pengguna yang mengakses API dan cara mereka mengakses API. Wawasan ini memungkinkan visibilitas aktivitas pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (h)	Jejak	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.
3.1 (h)	Jejak	codebuild-project-logging-enabled	Pastikan pencatatan AWS CodeBuild proyek diaktifkan sehingga log keluaran build Anda dikirim ke Amazon CloudWatch atau Amazon Simple Storage Service (Amazon S3). Log keluaran build memberikan informasi mendetail tentang proyek build Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (h)	Jalan setapak	opensearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktif kan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. OpenSearc h Log kesalahan layanan dapat membantu audit keamanan dan akses, dan dapat membantu mendiagno sis masalah ketersedi aan.
3.1 (h)	Jalan setapak	redshift-audit-logging-enabled	Untuk menangkap informasi tentang koneksi dan aktivitas pengguna di klaster Amazon Redshift, pastikan pencatatan audit diaktifkan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (h)	Jalan setapak	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penolakan dengan merekam tindakan AWS Management Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilkan, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
3.1 (h)	Jalan setapak	cloudtrail-s3-data events-diaktifkan	Pengumpulan peristiwa data Simple Storage Service (Amazon S3) membantu mendeteksi aktivitas anomali apa pun. Detailnya mencakup Akun AWS informasi yang mengakses bucket Amazon S3, alamat IP, dan waktu acara.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (h)	Jalan setapak	cw-loggroup-retention-period-periksa	Pastikan durasi minimum data log peristiwa disimpan untuk grup log Anda untuk membantu pemecahan masalah dan investigasi forensik. Kurangnya data log peristiwa masa lalu yang tersedia membuat sulit untuk merekonstruksi dan mengidentifikasi peristiwa yang berpotensi berbahaya.
3.1 (h)	Jalan setapak	elasticsearch-logs-to-cloudwatch	Pastikan domain OpenSearch Layanan Amazon mengaktifkan log kesalahan dan dialirkan ke CloudWatch Log Amazon untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (h)	Jalan setapak	elb-logging-enabled	Aktivitas Elastic Load Balancing adalah titik pusat komunikasi dalam suatu lingkungan. Pastikan pencatata n ELB diaktifkan. Data yang dikumpulk an memberikan informasi rinci tentang permintaan yang dikirim ke ELB. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (h)	Jalan setapak	multi-region-cloudtrail-enabled	AWS CloudTrail merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. CloudTrail akan mengirimkan file log dari semua AWS Wilayah ke bucket S3 Anda jika MULTI_REG ION_CLOUD _TRAIL_ENABLED diaktifkan. Selain itu, ketika AWS meluncurkan Wilayah baru, CloudTrail akan membuat jejak yang sama di Wilayah baru. Akibatnya, Anda akan menerima file log yang berisi aktivitas API untuk Wilayah baru tanpa mengambil tindakan apa pun.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (h)	Jalan setapak	rds-logging-enabled	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, pastikan pencatatan Amazon Relational Database Service (Amazon RDS) diaktifkan. Dengan pencatatan Amazon RDS, Anda dapat menangkap peristiwa seperti koneksi, pemutusan sambungan, kueri, atau tabel yang ditanyakan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (h)	Jalan setapak	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberikan rincian tentang permintaan akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (h)	Jalan setapak	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (h)	Jalan setapak	wafv2-logging-diaktifkan	Untuk membantu pencatatan dan pemantauan di lingkungan Anda, aktifkan pencatatan AWS WAF (V2) di web ACLs regional dan global. AWS Pencatatan WAF memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Log mencatat waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (h)	Jalan setapak	redshift-cluster-configuration-check	Untuk melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk klaster Amazon Redshift Anda. Anda juga harus memastikan bahwa konfigurasi yang diperlukan diterapkan di klaster Amazon Redshift. Pencatatan audit harus diaktifkan untuk memberikan informasi tentang koneksi dan aktivitas pengguna dalam database. Aturan ini mensyaratkan bahwa nilai ditetapkan untuk clusterDb Encrypted (Config Default: TRUE), dan LoggingEnabled (Config Default: TRUE). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (i)	Infrastruktur Kunci Publik	acm-certificate-expiration-check	Pastikan integritas jaringan dilindungi dengan memastikan sertifikat X509 dikeluarkan oleh AWS ACM. Sertifikat ini harus valid dan belum kedaluwarsa. Aturan ini membutuhkan nilai untuk daysToExpiration (Nilai Praktik Terbaik Keamanan AWS Dasar: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
3.1 (i)	Infrastruktur Kunci Publik	alb-http-drop-invalid-Header-diaktifkan	Pastikan Elastic Load Balancers (ELB) Anda dikonfigurasi untuk menjatuhkan header http. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (i)	Infrastruktur Kunci Publik	alb-http-to-https-pengalihan-periksa	Untuk membantu melindungi data dalam perjalana n, pastikan bahwa Application Load Balancer Anda secara otomatis mengalihk an permintaan HTTP yang tidak terenkrip si ke HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
3.1 (i)	Infrastruktur Kunci Publik	api-gw-ssl-enabled	Pastikan tahapan API REST API Amazon API Gateway dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengauten tikasi permintaan yang berasal dari API Gateway.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (i)	Infrastruktur Kunci Publik	opensearch-https-required	Karena data sensitif dapat ada dan membantu melindungi data dalam perjalanan, pastikan HTTPS diaktifkan untuk koneksi ke domain OpenSearch Layanan Amazon Anda.
3.1 (i)	Infrastruktur Kunci Publik	elbv2- acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifikat SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (i)	Infrastruktur Kunci Publik	elb-acm-certificate-required	Karena data sensitif dapat ada dan untuk membantu melindungi data saat transit, pastikan enkripsi diaktifkan untuk Elastic Load Balancing Anda. Gunakan AWS Certificate Manager untuk mengelola, menyediakan, dan menyebarkan sertifika t SSL/TLS publik dan pribadi dengan AWS layanan dan sumber daya internal.
3.1 (i)	Infrastruktur Kunci Publik	elb-tls-https-listeners-hanya	Pastikan Elastic Load Balancers (ELBs) Anda dikonfigurasi dengan pendengar SSL atau HTTPS. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.1 (i)	Infrastruktur Kunci Publik	redshift-require-tls-ssl	Pastikan klaster Amazon Redshift Anda memerlukan enkripsi TLS/SSL untuk terhubung ke klien SQL. Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.
3.1 (i)	Infrastruktur Kunci Publik	s3- bucket-ssl-requests-only	Untuk membantu melindungi data dalam perjalana n, pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda memerlukan permintaan untuk menggunakan Secure Socket Layer (SSL). Karena data sensitif dapat ada, aktifkan enkripsi dalam perjalanan untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Manajemen Kerentanan	elastic-beanstalk-managed-updates-diaktifkan	Mengaktifkan pembaruan platform terkelola untuk lingkungan Amazon Elastic Beanstalk memastikan bahwa perbaikan , pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah praktik terbaik dalam mengamankan sistem.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Manajemen Kerentanan	rds-automatic-minor-version-upgrade diaktifkan	Aktifkan upgrade versi minor otomatis pada instans Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS) untuk memastikan pembaruan versi minor terbaru ke Relational Database Management System (RDBMS) diinstal, yang mungkin mencakup patch keamanan dan perbaikan bug.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Manajemen Kerentanan	redshift-cluster-maintenancesettings-check	Aturan ini memastikan bahwa klaster Amazon Redshift memiliki pengaturan yang diinginkan untuk organisasi Anda. Secara khusus, bahwa mereka lebih menyukai jendela pemeliharaan dan periode retensi snapshot otomatis untuk database. Aturan ini mengharuskan Anda untuk mengatur allowVersionUpgrade. Bawaannya adalah benar. Ini juga memungkinkan Anda secara opsional mengatur preferredMaintenanceWindow (defaultnya adalah sat: 16:00-sat: 16:30), dan automatedSnapshotRetention Periode (defaultnya adalah 1). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Manajemen Kerentanan	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Manajemen Kerentanan	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Manajemen Kerentanan	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.3	Manajemen Kerentanan	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5	Rencana Manajemen Krisis Cyber	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5	Rencana Manajemen Krisis Cyber	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5	Rencana Manajemen Krisis Cyber	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisas i dimungkinkan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5	Rencana Manajemen Krisis Cyber	ec2- -periksa managedinstance-association-compliance-status	Gunakan Asosiasi AWS Systems Manager untuk membantu inventaris platform perangkat lunak dan aplikasi dalam suatu organisasi. AWS Systems Manager menetapkan status konfigurasi untuk instans terkelola Anda dan memungkinkan Anda untuk mengatur dasar tingkat patch sistem operasi, instalasi perangkat lunak, konfigurasi aplikasi, dan detail lainnya tentang lingkungan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.5	Rencana Manajemen Krisis Cyber	ec2- -periksa managedinstance-patch-compliance-status	Aktifkan aturan ini untuk membantu identifikasi dan dokumentasi kerentanan Amazon Elastic Compute Cloud (Amazon EC2). Aturan memeriksa apakah EC2 instans Amazon menambal kepatuhan di AWS Systems Manager sebagaimana diwajibkan oleh kebijakan dan prosedur organisasi Anda.
3.9	Penilaian Risiko TI	annual-risk-assessment-performed (pemeriksaan proses)	Lakukan penilaian risiko tahunan pada organisasi Anda. Penilaian risiko dapat membantu dalam menentukan kemungkinan dan dampak dari risiko dan/atau kerentanan yang diidentifikasi yang mempengaruhi suatu organisasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
3.12	Pelatihan	security-awareness -program-exists (pemeriksaan proses)	Membangun dan memelihara program kesadaran keamanan untuk organisas i Anda. Program kesadaran keamanan mendidik karyawan tentang cara melindungi organisas i mereka dari berbagai pelanggaran atau insiden keamanan.
4,4 (g)	Analisis penipuan - Analisis transaksi yang mencuriga kan, penggelap an, pencurian atau dugaan pencucian uang, penyalahgunaan aset, manipulasi catatan keuangan, dll. Persyaratan peraturan untuk melaporka n penipuan ke RBI harus didorong oleh sistem.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4,4 (h)	Analisis kapasitas dan kinerja sistem keamanan TI.	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4,4 (h)	Analisis kapasitas dan kinerja sistem keamanan TI.	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4,4 (h)	Analisis kapasitas dan kinerja sistem keamanan TI.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
4,4 (h)	Analisis kapasitas dan kinerja sistem keamanan TI.	clb-multiple-az	Elastic Load Balancing (ELB) secara otomatis mendistribusikan lalu lintas masuk Anda di beberapa target, seperti EC2 instance, kontainer, dan alamat IP, di zona ketersediaan. Untuk memastikan ketersediaan tinggi, pastikan ELB Anda telah mendaftarkan instans dari beberapa Availability Zone.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4,4 (h)	Analisis kapasitas dan kinerja sistem keamanan TI.	elbv2-multiple-az	Elastic Load Balancing (ELB) secara otomatis mendistribusikan lalu lintas masuk Anda di beberapa target, seperti EC2 instance, kontainer, dan alamat IP, di zona ketersedi aan. Untuk memastika n ketersediaan tinggi, pastikan ELB Anda telah mendaftarkan instans dari beberapa Availability Zone.
4,4 (h)	Analisis kapasitas dan kinerja sistem keamanan TI.	lambda-vpc-multi-az-periksa	Jika fungsi AWS Lambda Anda dikonfigurasi untuk terhubung ke virtual private cloud (VPC) di akun Anda, gunakan fungsi AWS Lambda di setidaknya dua Availability Zone yang berbeda untuk memastikan bahwa fungsi Anda tersedia untuk memproses peristiwa jika terjadi gangguan layanan di satu zona.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4,4 (h)	Analisis kapasitas dan kinerja sistem keamanan TI.	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4,4 (h)	Analisis kapasitas dan kinerja sistem keamanan TI.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4,4 (h)	Analisis kapasitas dan kinerja sistem keamanan TI.	s3- bucket-default-lock-enabled	Pastikan bucket Amazon Simple Storage Service (Amazon S3) Anda telah mengaktifkan kunci, secara default. Karena data sensitif dapat ada saat diam di bucket S3, terapkan kunci objek saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4,4 (h)	Analisis kapasitas dan kinerja sistem keamanan TI.	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4,4 (h)	Analisis kapasitas dan kinerja sistem keamanan TI.	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4,4 (h)	Analisis kapasitas dan kinerja sistem keamanan TI.	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
4,4 (h)	Analisis kapasitas dan kinerja sistem keamanan TI.	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.
4,4 (h)	Analisis kapasitas dan kinerja sistem keamanan TI.	lambda-concurrency-check	Aturan ini memastikan bahwa batas tinggi dan rendah konkurensi fungsi Lambda ditetapkan. Ini dapat membantu dalam menyusun dasar jumlah permintaan yang dilayani oleh fungsi Anda pada waktu tertentu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4,4 (h)	Analisis kapasitas dan kinerja sistem keamanan TI.	lambda-dlq-check	Aktifkan aturan ini untuk membantu memberi tahu personel yang sesuai melalui Amazon Simple Queue Service (Amazon SQS) atau Amazon Simple Notification Service (Amazon SNS) saat fungsi gagal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4,4 (h)	Analisis kapasitas dan kinerja sistem keamanan TI.	beanstalk-enhanced-health-reporting-diaktifkan	AWS Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi. Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4,4 (h)	Analisis kapasitas dan kinerja sistem keamanan TI.	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4,4 (h)	Analisis kapasitas dan kinerja sistem keamanan TI.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4,4 (h)	Analisis kapasitas dan kinerja sistem keamanan TI.	ebs-optimized-instance	Instans yang dioptimalkan di Amazon Elastic Block Store (Amazon EBS) menyediakan kapasitas tambahan dan khusus untuk operasi Amazon EBS I/O. Pengoptimalan ini memberikan kinerja paling efisien untuk volume EBS Anda dengan meminimalkan perselisihan antara operasi Amazon EBS I/O dan lalu lintas lain dari instans Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4,4 (h)	Analisis kapasitas dan kinerja sistem keamanan TI.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.4 (i)	Pelaporan insiden, dampaknya dan langkah-langkah yang diambil untuk tidak terulangnya peristiwa semacam itu di masa depan.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
4.4 (i)	Pelaporan insiden, dampaknya dan langkah-langkah yang diambil untuk tidak terulangnya peristiwa semacam itu di masa depan.	guardduty-non-archived-findings	Amazon GuardDuty membantu Anda memahami dampak insiden dengan mengklasifikasikan temuan berdasarkan tingkat keparahan : rendah, sedang, dan tinggi. Anda dapat menggunakan klasifikasi ini untuk menentukan strategi dan prioritas remediasi. Aturan ini memungkinkan Anda untuk secara opsional menyetel daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), dan daysHighSev (Config Default: 1) untuk temuan yang tidak diarsipkan, seperti yang disyaratkan oleh kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.3	NBFCs harus mempertimbangkan kebutuhan untuk menempatkan situs cadangan yang diperlukan untuk sistem bisnis penting dan pusat data mereka.	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.3	NBFCs harus mempertimbangkan kebutuhan untuk menempatkan situs cadangan yang diperlukan untuk sistem bisnis penting dan pusat data mereka.	aurora-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Aurora Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.3	NBFCs harus mempertimbangkan kebutuhan untuk menempatkan situs cadangan yang diperlukan untuk sistem bisnis penting dan pusat data mereka.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.3	NBFCs harus mempertimbangkan kebutuhan untuk menempatkan situs cadangan yang diperlukan untuk sistem bisnis penting dan pusat data mereka.	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.3	NBFCs harus mempertimbangkan kebutuhan untuk menempatkan situs cadangan yang diperlukan untuk sistem bisnis penting dan pusat data mereka.	cmk-backing-key-rotation-diaktifkan	Aktifkan rotasi kunci untuk memastikan bahwa kunci diputar setelah mencapai akhir periode crypto mereka.
6.3	NBFCs harus mempertimbangkan kebutuhan untuk menempatkan situs cadangan yang diperlukan untuk sistem bisnis penting dan pusat data mereka.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpanan instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkinkan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyaratan ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.3	NBFCs harus mempertimbangkan kebutuhan untuk menempatkan situs cadangan yang diperlukan untuk sistem bisnis penting dan pusat data mereka.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.3	NBFCs harus mempertimbangkan kebutuhan untuk menempatkan situs cadangan yang diperlukan untuk sistem bisnis penting dan pusat data mereka.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.3	NBFCs harus mempertimbangkan kebutuhan untuk menempatkan situs cadangan yang diperlukan untuk sistem bisnis penting dan pusat data mereka.	ec2- -rencana resources-protected-by-backup	Untuk membantu proses pencadangan data, pastikan sumber daya Amazon Elastic Compute Cloud EC2 (Amazon) Anda merupakan bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.3	NBFCs harus mempertimbangkan kebutuhan untuk menempatkan situs cadangan yang diperlukan untuk sistem bisnis penting dan pusat data mereka.	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.3	NBFCs harus mempertimbangkan kebutuhan untuk menempatkan situs cadangan yang diperlukan untuk sistem bisnis penting dan pusat data mereka.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.3	NBFCs harus mempertimbangkan kebutuhan untuk menempatkan situs cadangan yang diperlukan untuk sistem bisnis penting dan pusat data mereka.	fsx-resources-protected-by-rencana cadangan	Untuk membantu proses pencadangan data, pastikan sistem FSx file Amazon Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.3	NBFCs harus mempertimbangkan kebutuhan untuk menempatkan situs cadangan yang diperlukan untuk sistem bisnis penting dan pusat data mereka.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.3	NBFCs harus mempertimbangkan kebutuhan untuk menempatkan situs cadangan yang diperlukan untuk sistem bisnis penting dan pusat data mereka.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk cluster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
6.3	NBFCs harus mempertimbangkan kebutuhan untuk menempatkan situs cadangan yang diperlukan untuk sistem bisnis penting dan pusat data mereka.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.1	Sistem TI harus ditingkatkan secara progresif karena ukuran dan kompleksitas operasi NBFC meningkat.	dynamodb-autoscaling-enabled	Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application AWS Auto Scaling untuk menyesuaikan kapasitas throughput yang disediakan yang secara otomatis merespons pola lalu lintas aktual. Ini memungkinkan tabel atau indeks sekunder global untuk meningkatkan kapasitas baca/tulis yang disediakan untuk menangani peningkatan lalu lintas yang tiba-tiba, tanpa pembatasan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.1	Sistem TI harus ditingkatkan secara progresif karena ukuran dan kompleksitas operasi NBFC meningkat.	elb-cross-zone-load-menyeimbangkan diaktifkan	Aktifkan penyeimbangan beban lintas zona untuk Elastic Load Balancers (ELBs) Anda untuk membantu menjaga kapasitas dan ketersediaan yang memadai. Penyeimbangan beban lintas zona mengurangi kebutuhan untuk mempertahankan jumlah instance yang setara di setiap zona ketersediaan yang diaktifkan. Ini juga meningkatkan kemampuan aplikasi Anda untuk menangani hilangnya satu atau lebih instance.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.1	Sistem TI harus ditingkatkan secara progresif karena ukuran dan kompleksitas operasi NBFC meningkat.	elb-deletion-protection-enabled	Aturan ini memastikan bahwa Elastic Load Balancing memiliki perlindungan penghapusan yang diaktifkan. Gunakan fitur ini untuk mencegah penyeimbang beban Anda terhapus secara tidak sengaja atau jahat, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.
8.1	Sistem TI harus ditingkatkan secara progresif karena ukuran dan kompleksitas operasi NBFC meningkat.	clb-multiple-az	Elastic Load Balancing (ELB) secara otomatis mendistribusikan lalu lintas masuk Anda di beberapa target, seperti EC2 instance, kontainer, dan alamat IP, di zona ketersediaan. Untuk memastikan ketersediaan tinggi, pastikan ELB Anda telah mendaftarkan instans dari beberapa Availability Zone.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.1	Sistem TI harus ditingkatkan secara progresif karena ukuran dan kompleksitas operasi NBFC meningkat.	elbv2-multiple-az	Elastic Load Balancing (ELB) secara otomatis mendistribusikan lalu lintas masuk Anda di beberapa target, seperti EC2 instance, kontainer, dan alamat IP, di zona ketersediaan. Untuk memastikan ketersediaan tinggi, pastikan ELB Anda telah mendaftarkan instans dari beberapa Availability Zone.
8.1	Sistem TI harus ditingkatkan secara progresif karena ukuran dan kompleksitas operasi NBFC meningkat.	lambda-vpc-multi-az-periksa	Jika fungsi AWS Lambda Anda dikonfigurasi untuk terhubung ke virtual private cloud (VPC) di akun Anda, gunakan fungsi AWS Lambda di setidaknya dua Availability Zone yang berbeda untuk memastikan bahwa fungsi Anda tersedia untuk memproses peristiwa jika terjadi gangguan layanan di satu zona.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.1	Sistem TI harus ditingkatkan secara progresif karena ukuran dan kompleksitas operasi NBFC meningkat.	rds-instance-deletion-protection-diaktifkan	Pastikan instans Amazon Relational Database Service (Amazon RDS) mengaktifkan perlindungan penghapusan. Gunakan perlindungan penghapusan untuk mencegah instans Amazon RDS Anda dihapus secara tidak sengaja atau berbahaya, yang dapat menyebabkan hilangnya ketersediaan untuk aplikasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.1	Sistem TI harus ditingkatkan secara progresif karena ukuran dan kompleksitas operasi NBFC meningkat.	rds-multi-az-support	Dukungan multi-AZ di Amazon Relational Database Service (Amazon RDS) memberikan peningkatan ketersediaan dan daya tahan untuk instans database. Saat Anda menyediakan instans database Multi-AZ, Amazon RDS secara otomatis membuat instance database utama, dan mereplikasi data secara sinkron ke instans siaga di Availability Zone yang berbeda. Setiap Availability Zone berjalan pada infrastruktur independen yang berbeda secara fisik, dan direkayasa agar sangat andal. Jika terjadi kegagalan infrastruktur, Amazon RDS melakukan failover otomatis ke standby sehingga Anda dapat melanjutkan operasi database segera setelah failover selesai.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.1	Sistem TI harus ditingkatkan secara progresif karena ukuran dan kompleksitas operasi NBFC meningkat.	vpc-vpn-2-terowongan	Terowongan Site-to-Site VPN redundan dapat diimplementasikan untuk mencapai persyaratan ketahanan. Ini menggunakan dua terowongan untuk membantu memastikan konektivitas jika salah satu koneksi Site-to-Site VPN menjadi tidak tersedia. Untuk melindungi dari hilangnya konektivitas, jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua ke Amazon Virtual Private Cloud (Amazon VPC) dan gateway pribadi virtual dengan menggunakan gateway pelanggan kedua.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.1	Sistem TI harus ditingkatkan secara progresif karena ukuran dan kompleksitas operasi NBFC meningkat.	autoscaling-group-elb-healthcheck-diperlukan	Pemeriksaan kesehatan Elastic Load Balancer (ELB) untuk grup Auto EC2 Scaling Amazon Elastic Compute Cloud (Amazon) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. Penyeimbang beban secara berkala mengirimkan ping, mencoba koneksi, atau mengirim permintaan untuk menguji kesehatan EC2 instans Amazon dalam grup auto-scaling. Jika instans tidak melaporkan kembali, lalu lintas dikirim ke EC2 instans Amazon baru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.1	Sistem TI harus ditingkatkan secara progresif karena ukuran dan kompleksitas operasi NBFC meningkat.	dynamodb-throughput-limit-check	Aktifkan aturan ini untuk memastikan bahwa kapasitas throughput yang disediakan diperiksa di tabel Amazon DynamoDB Anda. Ini adalah jumlah aktivitas baca/tulis yang dapat didukung oleh setiap tabel. DynamoDB menggunakan informasi ini untuk mencadangkan sumber daya sistem yang memadai guna memenuhi persyaratan throughput Anda. Aturan ini menghasilkan peringatan ketika throughput mendekati batas maksimum untuk akun pelanggan. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter RCUThreshold Persentase akun (Config Default: 80) dan Persentase WCUThreshold

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			akun (Config Default: 80). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
8.1	Sistem TI harus ditingkatkan secara progresif karena ukuran dan kompleksi tas operasi NBFC meningkat.	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.1	Sistem TI harus ditingkatkan secara progresif karena ukuran dan kompleksitas operasi NBFC meningkat.	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.
8.1	Sistem TI harus ditingkatkan secara progresif karena ukuran dan kompleksitas operasi NBFC meningkat.	lambda-concurrency-check	Aturan ini memastikan bahwa batas tinggi dan rendah konkurensi fungsi Lambda ditetapkan. Ini dapat membantu dalam menyusun dasar jumlah permintaan yang dilayani oleh fungsi Anda pada waktu tertentu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.1	Sistem TI harus ditingkatkan secara progresif karena ukuran dan kompleksitas operasi NBFC meningkat.	rds-enhanced-monitoring-enabled	Aktifkan Amazon Relational Database Service (Amazon RDS) untuk membantu memantau ketersediaan Amazon RDS. Ini memberikan visibilitas terperinci ke dalam kesehatan instans database Amazon RDS Anda. Saat penyimpanan Amazon RDS menggunakan lebih dari satu perangkat fisik yang mendasarinya, Enhanced Monitoring mengumpulkan data untuk setiap perangkat. Selain itu, saat instans database Amazon RDS berjalan dalam penerapan multi-AZ, data untuk setiap perangkat di host sekunder dikumpulkan, dan metrik host sekunder.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.1	Sistem TI harus ditingkatkan secara progresif karena ukuran dan kompleksi tas operasi NBFC meningkat.	Securityhub-enabled	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	dms-replication-not-public	Kelola akses ke AWS Cloud dengan memastikan instans replikasi DMS tidak dapat diakses publik. Instans replikasi DMS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	ebs-snapshot-public-restorable-periksa	Kelola akses ke AWS Cloud dengan memastikan snapshot EBS tidak dapat dipulihkan secara publik. Snapshot volume EBS dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	elasticsearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan Domain OpenSearch Layanan Amazon (OpenSearch Layanan) berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan dalam VPC Amazon memungkinkan komunikasi yang aman antara OpenSearch Layanan dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	emr-master-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan node master cluster EMR Amazon tidak dapat diakses publik. Node master cluster EMR Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	terbatas-ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	lambda-function-public-access-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyaratan untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibanding kan dengan domain yang menggunak an titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	rds-instance-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi sensitif, dan prinsip serta kontrol akses diperlukan untuk akun tersebut.
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	rds-snapshots-public-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa instans Amazon Relational Database Service (Amazon RDS) tidak bersifat publik. Instans database Amazon RDS dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	redshift-cluster-public-access-periksa	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa klaster Amazon Redshift tidak bersifat publik. Cluster Amazon Redshift dapat berisi informasi dan prinsip sensitif dan kontrol akses diperlukan untuk akun tersebut.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Aturan ini memungkinkan Anda untuk secara opsional mengatur parameter BlockedPo rt1 - BlockedPort5 (Config Defaults: 20,21,3389,3306,43 33). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	s3- bucket-public-read -prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	s3- bucket-public-writ e-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	sagemaker-notebook-no-direct-akses internet	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa SageMaker notebook Amazon tidak mengizinkan akses internet langsung. Dengan mencegah akses internet langsung, Anda dapat menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediak an pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integrita s, dan kerahasia an sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	access-keys-rotated	Kredensyal diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaimana ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	emr-kerberos-enabled	Izin akses dan otorisasi dapat dikelola dan digabungkan dengan prinsip-prinsip hak istimewa dan pemisahan tugas, dengan mengaktif kan Kerberos untuk cluster EMR Amazon. Di Kerberos, layanan dan pengguna yang perlu mengauten tikasi dikenal sebagai prinsipal. Prinsipal ada di dalam ranah Kerberos. Di dunia, server Kerberos dikenal sebagai pusat distribusi kunci (KDC). Ini menyediak an sarana bagi kepala sekolah untuk mengotentikasi. KDC mengautentikasi dengan mengeluar kan tiket untuk otentikasi. KDC mempertahankan basis data utama dari ranah, kata sandi mereka, dan informasi administratif lainnya tentang setiap utama.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	autoscaling-launch-config-public-ip-dinonaktifkan	Jika Anda mengonfigurasi Antarmuka Jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan Antarmuka Jaringan tersebut dapat dijangkau dari internet. EC2 sumber daya tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke aplikasi atau server Anda.
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	ec2- instance-profile-attached	EC2 profil instance meneruskan peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya pada tindakan yang diperlukan. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	ecs-task-definition-nonroot-pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan bahwa pengguna non-root ditunjuk untuk mengakses definisi tugas Amazon Elastic Container Service (Amazon ECS) Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	efs-access-point-enforce-root-direktori	Menegakkan direktori root untuk jalur akses Amazon Elastic File System (Amazon EFS) membantu membatasi akses data dengan memastikan bahwa pengguna jalur akses hanya dapat menjangkau file dari subdirektori yang ditentukan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	efs-access-point-enforce-identitas pengguna	Untuk membantu menerapkan prinsip hak istimewa paling sedikit, pastikan penegakan pengguna diaktifkan untuk Amazon Elastic File System (Amazon EFS) Anda. Saat diaktifkan, Amazon EFS mengganti kan pengguna dan grup klien NFS IDs dengan identitas yang dikonfigurasi pada titik akses untuk semua operasi sistem file dan hanya memberika n akses ke identitas pengguna yang diberlakukan ini.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	s3- bucket-acl-prohibited	Aturan ini memeriksa untuk melihat apakah Daftar Kontrol Akses (ACLs) digunakan untuk kontrol akses di Bucket Amazon S3. ACLs adalah mekanisme kontrol akses lama untuk bucket Amazon S3 yang AWS mendahului Identity and Access Management (IAM). Sebagai gantinya ACLs, ini adalah praktik terbaik untuk menggunakan kebijakan IAM atau kebijakan bucket S3 untuk mengelola akses ke bucket S3 Anda dengan lebih mudah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	s3- -dilarang bucket-level-public-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspos informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	subnet-auto-assign-public-ip-dinonaktifkan	Kelola akses ke AWS Cloud dengan memastikan subnet Amazon Virtual Private Cloud (VPC) tidak secara otomatis ditetapkan alamat IP publik. Instans Amazon Elastic Compute Cloud (EC2) yang diluncurkan ke subnet yang mengaktifkan atribut ini memiliki alamat IP publik yang ditetapkan ke antarmuka jaringan utamanya.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Managemen t (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas terkecil.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifkan untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredensyal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsageUsia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindun gan ekstra di atas kredensyal masuk. Dengan mewajibka n MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	root-account-hardware-mfa-diaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensyal masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	opensearch-in-vpc-only	Kelola akses ke AWS Cloud dengan memastikan domain OpenSearch Layanan Amazon berada dalam Amazon Virtual Private Cloud (Amazon VPC). Domain OpenSearch Layanan Amazon dalam VPC Amazon memungkin kan komunikasi yang aman antara OpenSearch Layanan Amazon dan layanan lain dalam VPC Amazon tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahkan lapisan perlindungan ekstra untuk kredensyal masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	secretsmanager-rotation-enabled-check	Aturan ini memastikan AWS rahasia Secrets Manager telah diaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. I	Aspek keamanan dasar seperti kontrol akses fisik/logis dan kebijakan kata sandi yang terdefinisi dengan baik.	secretsmanager-scheduled-rotation-success-periksa	Aturan ini memastikan bahwa AWS rahasia Secrets Manager telah berhasil diputar sesuai dengan jadwal rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode di mana rahasia aktif, dan berpotensi mengurangi dampak bisnis jika dikompromikan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.II	Peran pengguna yang terdefinisi dengan baik.	iam-group-has-users-periksa	AWS Identity and Access Managemen t (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastika n bahwa grup IAM memiliki setidakny a satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.II	Peran pengguna yang terdefinisi dengan baik.	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Managemen t (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkin kan penggunaan kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.II	Peran pengguna yang terdefinisi dengan baik.	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyaratan sebagaimana dinyatakan oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCharacters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
			(Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPasswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordReusePrevention MaxPasswordAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.II	Peran pengguna yang terdefinisi dengan baik.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandung “Efek”: “Izinkan” dengan “Tindakan”: “*” di atas “Sumber Daya”: “*”. Memungkinkan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.II	Peran pengguna yang terdefinisi dengan baik.	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi, dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.II	Peran pengguna yang terdefinisi dengan baik.	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontrol akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurangi peluang bagi identitas untuk menerima atau mempertahankan hak istimewa yang berlebihan.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.II	Peran pengguna yang terdefinisi dengan baik.	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensyal yang tidak digunakan ini diidentifikasi, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsageUsia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8.III	Konsep Maker-Checker untuk mengurangi risiko kesalahan dan penyalahgunaan dan untuk memastikan keandalan data/informasi.	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. IX	Pengaturan untuk cadangan data dengan pengujian berkala.	db-instance-backup-enabled	Fitur cadangan Amazon RDS membuat cadangan database dan log transaksi Anda. Amazon RDS secara otomatis membuat snapshot volume penyimpan an instans DB Anda, mencadangkan seluruh instans DB. Sistem ini memungkin kan Anda untuk mengatur periode retensi tertentu untuk memenuhi persyarat an ketahanan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. IX	Pengaturan untuk cadangan data dengan pengujian berkala.	dynamodb-in-backup-plan	Untuk membantu proses pencadangan data, pastikan tabel Amazon DynamoDB Anda adalah bagian dari AWS paket Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. IX	Pengaturan untuk cadangan data dengan pengujian berkala.	dynamodb-pitr-enabled	Aktifkan aturan ini untuk memeriksa bahwa informasi telah dicadangkan. Ini juga mempertahankan cadangan dengan memastikan bahwa point-in-time pemulihan diaktifkan di Amazon DynamoDB. Pemulihan mempertahankan pencadangan berkelanjutan dari tabel Anda selama 35 hari terakhir.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. IX	Pengaturan untuk cadangan data dengan pengujian berkala.	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. IX	Pengaturan untuk cadangan data dengan pengujian berkala.	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. IX	Pengaturan untuk cadangan data dengan pengujian berkala.	elasticache-redis-cluster-automatic-backup-periksa	Saat pencadangan otomatis diaktifkan, Amazon ElastiCache membuat cadangan cluster setiap hari. Cadangan dapat disimpan selama beberapa hari seperti yang ditentukan oleh organisasi Anda. Pencadang an otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat cluster baru, yang mengembalikan data Anda dari cadangan terbaru.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. IX	Pengaturan untuk cadangan data dengan pengujian berkala.	rds-in-backup-plan	Untuk membantu proses pencadangan data, pastikan instans Amazon Relationa l Database Service (Amazon RDS) Anda adalah bagian dari paket Backup. AWS AWS Backup adalah layanan pencadang an yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederh anakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyarat an kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. IX	Pengaturan untuk cadangan data dengan pengujian berkala.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) mendukung pemeliharaan kapasitas dan ketersediaan yang memadai. CRR memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket Amazon S3 untuk membantu memastikan ketersedi aan data tetap terjaga.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. IX	Pengaturan untuk cadangan data dengan pengujian berkala.	redshift-backup-enabled	Untuk membantu proses pencadangan data, pastikan klaster Amazon Redshift Anda memiliki snapshot otomatis. Saat snapshot otomatis diaktifkan untuk cluster, Redshift secara berkala mengambil snapshot dari cluster tersebut. Secara default, Redshift mengambil snapshot setiap delapan jam atau setiap 5 GB untuk setiap node perubahan data, atau mana yang lebih dulu.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. IX	Pengaturan untuk cadangan data dengan pengujian berkala.	backup-plan-min-frequency-and-min-retention-check	Untuk membantu proses pencadangan data, pastikan paket AWS Backup diatur untuk frekuensi dan retensi minimum. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) dan (requiredFrequencyUnit Config default: days). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. IX	Pengaturan untuk cadangan data dengan pengujian berkala.	backup-recovery-point-manual-penghapusan-dinonaktifkan	Pastikan bahwa titik pemulihan AWS Backup Anda memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan . Menggunakan kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan dapat membantu mencegah penghapusan yang tidak disengaja atau disengaja.

ID Kontrol	Deskripsi Kontrol	AWS Aturan Config	Bimbingan
8. IX	Pengaturan untuk cadangan data dengan pengujian berkala.	backup-recovery-point-minimum-pemeriksaan retensi	Untuk membantu proses pencadangan data, pastikan titik pemulihan AWS Backup Anda memiliki periode retensi minimum yang ditetapkan. AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. Aturan ini memungkinkan Anda untuk mengatur parameter requiredRetentionDays (config default: 35). Nilai aktual harus mencerminkan persyaratan organisasi Anda.

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk RBI MD-ITF.

Praktik Terbaik Operasional untuk Layanan Keamanan, Identitas, dan Kepatuhan

Paket kesesuaian ini berisi AWS Config aturan berdasarkan Layanan Keamanan, Identitas, dan Kepatuhan. Untuk informasi selengkapnya, lihat Keamanan, Identitas, dan Kepatuhan di AWS. Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Layanan Keamanan, Identitas, dan Kepatuhan.

Praktik Terbaik Operasional untuk Tanpa Server

Paket kesesuaian ini berisi AWS Config aturan berdasarkan solusi Tanpa Server. Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Tanpa Server.

Praktik Terbaik Operasional untuk Layanan Penyimpanan

Paket kesesuaian ini berisi AWS Config aturan berdasarkan Layanan Penyimpanan. Untuk informasi selengkapnya, lihat Cloud Storage aktif AWS. Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Operasional untuk Layanan Penyimpanan.

Praktik Terbaik Operasional untuk SWIFT CSP

Paket kesesuaian menyediakan kerangka kerja kepatuhan tujuan umum yang dirancang untuk memungkinkan Anda membuat pemeriksaan tata kelola keamanan, operasional, atau pengoptimalan biaya menggunakan aturan dan tindakan remediasi terkelola atau khusus. AWS Config AWS Config Paket Kesesuaian, sebagai contoh templat, tidak dirancang untuk sepenuhnya memastikan kepatuhan terhadap tata kelola atau standar kepatuhan tertentu. Anda bertanggung jawab untuk membuat penilaian sendiri tentang apakah penggunaan Layanan oleh Anda memenuhi persyaratan hukum dan peraturan yang berlaku.

Berikut ini menyediakan contoh pemetaan antara Program Keamanan Pelanggan (CSP) SWIFT dan aturan AWS Config terkelola. Setiap AWS Config aturan berlaku untuk AWS sumber daya tertentu, dan berhubungan dengan satu atau lebih kontrol CSP SWIFT. Kontrol CSP SWIFT dapat dikaitkan dengan beberapa AWS Config aturan. Lihat tabel di bawah ini untuk detail lebih lanjut dan panduan terkait pemetaan ini.

ID Kontrol	AWS Aturan Config	Bimbingan
1.1	ec2- -manajer instance-managed-by-systems	Inventarisasi platform perangkat lunak dan aplikasi dalam organisasi dimungkin kan dengan mengelola instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Systems Manager. Gunakan AWS Systems Manager untuk menyediakan konfigurasi sistem terperinci, tingkat patch sistem operasi, nama dan jenis layanan, instalasi perangkat lunak, nama aplikasi, penerbit dan versi, dan detail lainnya tentang lingkungan Anda.
1.1	ec2- instance-no-public-ip	Kelola akses ke AWS Cloud dengan memastikan instans Amazon Elastic Compute

ID Kontrol	AWS Aturan Config	Bimbingan
		Cloud (Amazon EC2) tidak dapat diakses publik. EC2 Instans Amazon dapat berisi informasi sensitif dan kontrol akses diperlukan untuk akun tersebut.
1.1	ec2- no-amazon-key-pair	Aturan ini memeriksa apakah menjalankan instans Amazon Elastic Compute Cloud (Amazon EC2) diluncurkan menggunakan pasangan kunci amazon. Ini dapat membantu mengurangi risiko kredensi yang dikomprom ikan. EC2 Instans Amazon tanpa pasangan kunci masih dapat diakses menggunakan Pengelola Sesi atau koneksi SSH berbasis Browser dari konsol. AWS

ID Kontrol	AWS Aturan Config	Bimbingan
1.1	ec2- instances-in-vpc	Terapkan instans Amazon Elastic Compute Cloud (Amazon EC2) dalam Amazon Virtual Private Cloud (Amazon VPC) untuk memungkinkan komunikasi aman antara instans dan layanan lain dalam VPC amazon, tanpa memerlukan gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Tetapkan EC2 instans Amazon ke VPC Amazon untuk mengelola akses dengan benar.

ID Kontrol	AWS Aturan Config	Bimbingan
1.1	vpc-default-security-group-tertutup	Grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu dalam pengelola an akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Membatasi semua lalu lintas pada grup keamanan default membantu membatasi akses jarak jauh ke sumber daya Anda AWS .
1.1	vpc-network-acl-unused-periksa	Aturan ini memastikan bahwa daftar kontrol akses jaringan Amazon Virtual Private Cloud (VPC) sedang digunakan . Pemantauan untuk daftar kontrol akses jaringan yang tidak digunakan dapat membantu inventaris dan pengelolaan lingkungan Anda yang akurat.

ID Kontrol	AWS Aturan Config	Bimbingan
1.1	vpc-sg-open-only-to-authorized-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses pada port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Dengan membatasi akses ke sumber daya dalam kelompok keamanan dari internet (0.0.0.0/0) akses jarak jauh dapat dikontrol ke sistem internal.

ID Kontrol	AWS Aturan Config	Bimbingan
1.2	iam-customer-policy-blocked-kms-tindakan	AWS Identity and Access Management (IAM) dapat membantu Anda menggabun gkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, membatasi kebijakan agar tidak mengandun g tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS Memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesa ikan tugas dapat melanggar prinsip hak istimewa yang paling sedikit dan pemisahan tugas. Aturan ini memungkin kan Anda untuk mengatur blockedActionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda

ID Kontrol	AWS Aturan Config	Bimbingan
1.2	iam-group-has-users-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda menggabungkan prinsip-prinsip hak istimewa dan pemisahan tugas dengan izin akses dan otorisasi, dengan memastikan bahwa grup IAM memiliki setidaknya satu pengguna. Menempatkan pengguna dalam grup berdasarkan izin terkait atau fungsi pekerjaan adalah salah satu cara untuk memasukkan hak istimewa paling sedikit.

ID Kontrol	AWS Aturan Config	Bimbingan
1.2	iam-inline-policy-blocked-kms-tindakan	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM, atau grup IAM tidak memiliki kebijakan inline untuk mengizink an tindakan yang diblokir pada semua kunci Layanan Manajemen Kunci. AWS AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi, pengembalian, dan pendelega sian manajemen izin. Aturan ini memungkinkan Anda untuk mengatur blockedAc tionsPatterns parameter. (Nilai Praktik Terbaik Keamanan AWS Dasar: kms: Dekripsi,). kms: ReEncryptFrom Nilai aktual harus mencerminkan kebijakan organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1.2	iam-no-inline-policy-periksa	Pastikan pengguna AWS Identity and Access Management (IAM) and Access Management (IAM), peran IAM atau grup IAM tidak memiliki kebijakan inline untuk mengontrol akses ke sistem dan aset. AWS merekomendasikan untuk menggunakan kebijakan terkelola alih-alih kebijakan inline. Kebijakan terkelola memungkinkan penggunaa n kembali, pembuatan versi dan pemutaran kembali, serta mendelegasikan manajemen izin.
1.2	iam-user-no-policies-periksa	Aturan ini memastikan kebijakan AWS Identity and Access Management (IAM) dilampirkan hanya pada grup atau peran untuk mengontro l akses ke sistem dan aset. Menetapkan hak istimewa di kelompok atau tingkat peran membantu mengurang i peluang bagi identitas untuk menerima atau mempertah ankan hak istimewa yang berlebihan.

ID Kontrol	AWS Aturan Config	Bimbingan
1.2	dibatasi ssh	Grup Keamanan Amazon Elastic Compute Cloud (Amazon EC2) dapat membantu mengelola akses jaringan dengan menyediakan pemfilteran stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Tidak mengizinkan lalu lintas masuk (atau jarak jauh) dari 0.0.0.0/0 ke port 22 pada sumber daya Anda membantu Anda membatasi akses jarak jauh.
1.2	nacl-no-unrestricted-ssh-rdp	Akses ke port administrasi server jarak jauh di Daftar Kontrol Akses Jaringan Anda (NACLs), seperti port 22 (SSH) dan port 3389 (RDP), tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke sumber daya dalam VPC Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
1.2	s3- bucket-acl-prohibited	Aturan ini memeriksa untuk melihat apakah Daftar Kontrol Akses (ACLs) digunakan untuk kontrol akses di Bucket Amazon S3. ACLs adalah mekanisme kontrol akses lama untuk bucket Amazon S3 yang AWS mendahului Identity and Access Managemen t (IAM). Sebagai gantinya ACLs, ini adalah praktik terbaik untuk menggunakan kebijakan IAM atau kebijakan bucket S3 untuk mengelola akses ke bucket S3 Anda dengan lebih mudah.

ID Kontrol	AWS Aturan Config	Bimbingan
1.2	s3- bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) pencatatan akses server menyediakan metode untuk memantau jaringan untuk potensi peristiwa keamanan siber. Acara dipantau dengan menangkap catatan terperinci untuk permintaan yang dibuat ke bucket Amazon S3. Setiap catatan log akses memberika n rincian tentang permintaa n akses tunggal. Detailnya mencakup pemohon, nama bucket, waktu permintaan, tindakan permintaan, status respons, dan kode kesalahan, jika relevan.
1.2	s3- bucket-policy-grantee-check	Kelola akses ke AWS Cloud dengan mengaktifkan s3_ bucket_policy_grantee_check. Aturan ini memastikan bahwa akses yang diberikan oleh bucket Amazon S3 dibatasi oleh AWS prinsipal, pengguna federasi, kepala layanan, alamat IP, atau Amazon Virtual Private Cloud (Amazon VPC) yang Anda sediakan. IDs

ID Kontrol	AWS Aturan Config	Bimbingan
1.2	sns-topic-message-delivery-notifikasi-diaktifkan	Untuk membantu persyaratan pencatatan di lingkungan Anda, pastikan untuk mengaktifkan notifikasi status pengiriman diaktifkan untuk topik Simple Notification Service Amazon (Amazon SNS). Mencatat status pengiriman pesan membantu memberikan wawasan operasional yang lebih baik, seperti berikut ini: Mengetahui apakah pesan dikirim ke titik akhir Amazon SNS, mengidentifikasi respons yang dikirim dari titik akhir Amazon SNS ke Amazon SNS, dan menentukan waktu tinggal pesan (waktu antara stempel waktu publikasi dan sebelum menyerahkan ke titik akhir Amazon SNS).
1.4	internet-gateway-authorized-vpc-hanya	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa gateway internet hanya dilampirkan ke Amazon Virtual Private Cloud (Amazon VPC) resmi. Gateway internet memungkinkan akses internet dua arah ke dan dari VPC Amazon yang berpotensi menyebabkan akses tidak sah ke sumber daya VPC Amazon.

ID Kontrol	AWS Aturan Config	Bimbingan
1.4	restricted-common-ports	Kelola akses ke sumber daya di AWS Cloud dengan memastikan port umum dibatasi pada grup keamanan Amazon Elastic Compute Cloud (Amazon EC2). Tidak membatasi akses ke port ke sumber tepercaya dapat menyebabkan serangan terhadap ketersediaan, integritas, dan kerahasiaan sistem. Aturan ini memungkin kan Anda untuk secara opsional mengatur parameter BlockedPort1 - BlockedPort5 (Config Defaults: 20,21,338 9,3306,4333). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
1.4	lambda-function-public-acce ss-dilarang	Kelola akses ke sumber daya di AWS Cloud dengan memastikan fungsi AWS Lambda tidak dapat diakses secara publik. Akses publik berpotensi menyebabkan degradasi ketersediaan sumber daya.

ID Kontrol	AWS Aturan Config	Bimbingan
1.4	s3- account-level-public-access -blok-periodik	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik. Aturan ini memungkinkan Anda untuk secara opsional mengatur ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True), (Config Default: True), dan restrictPublicBuckets parameter blockPublicAcls (Config Default: True). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
1.4	s3- -dilarang bucket-level-publi c-access	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa bucket Amazon Simple Storage Service (Amazon S3) tidak dapat diakses publik. Aturan ini membantu menjaga keamanan data sensitif dari pengguna jarak jauh yang tidak sah dengan mencegah akses publik di tingkat bucket.

ID Kontrol	AWS Aturan Config	Bimbingan
1.4	s3- bucket-public-read-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
1.4	s3- bucket-public-write-prohibited	Kelola akses ke sumber daya di AWS Cloud dengan hanya mengizinkan pengguna, proses, dan perangkat yang berwenang mengakses bucket Amazon Simple Storage Service (Amazon S3). Pengelolaan akses harus konsisten dengan klasifikasi data.
1.4	ssm-document-not-public	Pastikan dokumen AWS Systems Manager (SSM) tidak bersifat publik, karena ini memungkinkan akses yang tidak diinginkan ke dokumen SSM Anda. Dokumen SSM publik dapat mengekspo s informasi tentang akun, sumber daya, dan proses internal Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.3	ec2-imdsv2-periksa	Pastikan metode Instance Metadata Service Version 2 (IMDSv2) diaktifkan untuk membantu melindungi akses dan kontrol metadata instans Amazon Elastic Compute Cloud (Amazon EC2). IMDSv2 Metode ini menggunak an kontrol berbasis sesi. Dengan IMDSv2, kontrol dapat diimplementasikan untuk membatasi perubahan pada metadata instance.
2.3	ec2- instance-multiple-eni-check	Aturan ini memeriksa apakah instans Amazon Elastic Compute Cloud (Amazon EC2) Anda memiliki beberapa. ENIs Memiliki beberapa ENIs dapat menyebabkan instance dual-homed, yang berarti instance yang memiliki beberapa subnet. Ini dapat menambah kompleksitas keamanan jaringan dan memperkenalkan jalur dan akses jaringan yang tidak diinginkan.

ID Kontrol	AWS Aturan Config	Bimbingan
2.3	ec2- token-hop-limit-check	Pastikan respons PUT HTTP Instance Metadata Service (IMDS) dibatasi pada instans Amazon Elastic Compute Cloud (Amazon). EC2 Dengan IMDSv2, respons PUT yang berisi token rahasia secara default tidak dapat berjalan di luar instance, karena batas hop respons Metadata diatur ke 1 (Config default). Jika nilai ini lebih besar dari 1, token dapat meninggalkan EC2 instance.
2.3	ec2- volume-inuse-check	Aturan ini memastikan bahwa volume Amazon Elastic Block Store yang dilampirk an ke instans Amazon Elastic Compute Cloud (Amazon EC2) ditandai untuk dihapus saat instance dihentikan. Jika volume Amazon EBS tidak dihapus ketika instance yang dilampirkan dihentikan, itu mungkin melanggar konsep fungsionalitas terkecil.

ID Kontrol	AWS Aturan Config	Bimbingan
2.3	account-part-of-organizations	Manajemen terpusat Akun AWS dalam AWS Organizat ions membantu memastika n bahwa akun sesuai. Kurangnya tata kelola akun terpusat dapat menyebabk an konfigurasi akun yang tidak konsisten, yang dapat mengekspos sumber daya dan data sensitif.
2.3	lambda-inside-vpc	Menerapkan fungsi AWS Lambda dalam Amazon Virtual Private Cloud (Amazon VPC) untuk komunikasi yang aman antara fungsi dan layanan lain dalam Amazon VPC. Dengan konfigura si ini, tidak ada persyarat an untuk gateway internet, perangkat NAT, atau koneksi VPN. Semua lalu lintas tetap aman di dalam AWS Cloud. Karena isolasi logisnya, domain yang berada di dalam VPC Amazon memiliki lapisan keamanan ekstra jika dibandingkan dengan domain yang menggunakan titik akhir publik. Untuk mengelola akses dengan benar, fungsi AWS Lambda harus ditetapkan ke VPC.

ID Kontrol	AWS Aturan Config	Bimbingan
2.3	kms-cmk-not-scheduled-untuk-penghapusan	Untuk membantu melindungi data saat istirahat, pastikan kunci master pelanggan yang diperlukan (CMKs) tidak dijadwalkan untuk dihapus di Layanan Manajemen AWS Kunci (AWS KMS). Karena penghapusan kunci diperlukan pada waktu tertentu, aturan ini dapat membantu dalam memeriksa semua kunci yang dijadwalkan untuk dihapus, jika kunci dijadwalkan secara tidak sengaja.
2.3	s3- bucket-versioning-enabled	Pembuatan versi bucket Amazon Simple Storage Service (Amazon S3) membantu menyimpan beberapa varian objek dalam bucket Amazon S3 yang sama. Gunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Amazon S3 Anda. Pembuatan versi membantu Anda memulihkan dengan mudah dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

ID Kontrol	AWS Aturan Config	Bimbingan
2.3	secretsmanager-secret-unused	Jika kredensil yang tidak digunakan ada di AWS Secrets Manager, Anda harus menonaktifkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini memungkinkan Anda untuk menetapkan nilai ke unusedForDays (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
2.5A	ebs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan volume Amazon Elastic Block Store (Amazon EBS) merupakan bagian dari paket Backup. AWS AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya dengan solusi pencadangan berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.5A	ec2- ebs-encryption-by-default	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS). Karena data sensitif dapat ada saat diam dalam volume ini, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.
2.5A	efs-encrypted-check	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Elastic File System (EFS) Anda.
2.5A	efs-in-backup-plan	Untuk membantu proses pencadangan data, pastikan sistem file Amazon Elastic File System (Amazon EFS) Anda adalah bagian dari paket AWS Backup. AWS Backup adalah layanan pencadang an yang dikelola sepenuhny a dengan solusi pencadang an berbasis kebijakan. Solusi ini menyederhanakan manajemen cadangan Anda dan memungkinkan Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
2.5A	volume terenkripsi	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk volume Amazon Elastic Block Store (Amazon EBS) Anda.
2.5A	kinesis-stream-encrypted	Karena data sensitif dapat ada dan membantu melindungi data saat istirahat, pastikan enkripsi diaktifkan untuk Amazon Kinesis Streams Anda.
2.5A	s3- -diaktifkan bucket-server-side-encryption	Untuk membantu melindung i data saat istirahat, pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi untuk membantu melindungi data tersebut.
2.5A	s3- default-encryption-kms	Pastikan enkripsi diaktifkan untuk bucket Amazon Simple Storage Service (Amazon S3). Karena data sensitif dapat ada saat diam di bucket Amazon S3, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
2.5A	sns-encrypted-kms	Untuk membantu melindung i data saat istirahat, pastikan topik Amazon Simple Notificat ion Service (Amazon SNS) Anda memerlukan enkripsi AWS menggunakan Key Management Service AWS (KMS). Karena data sensitif dapat ada saat diam dalam pesan yang dipublikasikan, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
4.1	iam-password-policy	Identitas dan kredensialnya dikeluarkan, dikelola, dan diverifikasi berdasarkan kebijakan kata sandi IAM organisasi. Mereka memenuhi atau melampaui persyarat an sebagaimana dinyataka n oleh NIST SP 800-63 dan standar Praktik Terbaik Keamanan AWS Dasar untuk kekuatan kata sandi. Aturan ini memungkinkan Anda untuk mengatur secara opsional RequireUppercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireLowercaseCh aracters (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireSymbols (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), RequireNumbers (Nilai Praktik Terbaik Keamanan AWS Dasar: benar), MinimumPa sswordLength (Nilai Praktik Terbaik Keamanan AWS Dasar: 14), (Nilai Praktik Terbaik Keamanan AWS Dasar: 24), dan PasswordR eusePrevention MaxPasswo rdAge (Nilai Praktik Terbaik Keamanan AWS Dasar: 90) untuk IAM Anda Kebijakan

ID Kontrol	AWS Aturan Config	Bimbingan
		Kata Sandi. Nilai aktual harus mencerminkan kebijakan organisasi Anda.
4.1	access-keys-rotated	Kredensi diaudit untuk perangkat, pengguna, dan proses yang berwenang dengan memastikan kunci akses IAM diputar sebagaima na ditentukan oleh kebijakan organisasi. Mengubah kunci akses pada jadwal reguler adalah praktik terbaik keamanan. Ini mempersingkat periode kunci akses aktif dan mengurangi dampak bisnis jika kunci dikompromikan. Aturan ini memerlukan nilai rotasi kunci akses (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
4.2	iam-user-mfa-enabled	Aktifkan aturan ini untuk membatasi akses ke sumber daya di AWS Cloud. Aturan ini memastikan otentikasi multi-faktor (MFA) diaktifka n untuk semua pengguna. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Kurangi insiden akun yang disusupi dengan mewajibkan MFA untuk pengguna.

ID Kontrol	AWS Aturan Config	Bimbingan
4.2	mfa-enabled-for-iam-akses konsol	Kelola akses ke sumber daya di AWS Cloud dengan memastikan bahwa MFA diaktifkan untuk semua pengguna AWS Identity and Access Management (IAM) and Access Management (IAM) yang memiliki kata sandi konsol. MFA menambahkan lapisan perlindungan ekstra di atas kredenal masuk. Dengan mewajibkan MFA untuk pengguna, Anda dapat mengurangi insiden akun yang disusupi dan menjaga agar data sensitif tidak diakses oleh pengguna yang tidak sah.
4.2	root-account-hardware-mfa-d iaktifkan	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA perangkat keras diaktifkan untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS

ID Kontrol	AWS Aturan Config	Bimbingan
4.2	root-account-mfa-enabled	Kelola akses ke sumber daya di AWS Cloud dengan memastikan MFA diaktifka n untuk pengguna root. Pengguna root adalah pengguna yang paling istimewa dalam file Akun AWS. MFA menambahk an lapisan perlindungan ekstra untuk kredensi masuk. Dengan mewajibkan MFA untuk pengguna root, Anda dapat mengurangi insiden yang disusupi. Akun AWS
5.1	ec2- instance-profile-attached	EC2 profil instance meneruska n peran IAM ke sebuah EC2 instance. Melampirkan profil instans ke instans Anda dapat membantu pengelolaan hak istimewa dan izin paling sedikit.
5.1	iam-policy-no-statements-with-full-access	Pastikan Tindakan IAM dibatasi hanya untuk tindakan yang diperlukan. Memungkin kan pengguna untuk memiliki lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
5.1	iam-root-access-key-periksa	Akses ke sistem dan aset dapat dikontrol dengan memeriksa bahwa pengguna root tidak memiliki kunci akses yang melekat pada peran AWS Identity and Access Management (IAM) mereka. Pastikan kunci akses root dihapus. Sebaliknya, buat dan gunakan berbasis peran Akun AWS untuk membantu menggabungkan prinsip fungsionalitas paling sedikit.
5.1	iam-user-group-membership-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda membatasi izin akses dan otorisasi , dengan memastikan pengguna adalah anggota setidaknya satu grup. Mengizinkan pengguna lebih banyak hak istimewa daripada yang dibutuhkan untuk menyelesaikan tugas dapat melanggar prinsip hak istimewa paling sedikit dan pemisahan tugas.

ID Kontrol	AWS Aturan Config	Bimbingan
5.1	iam-user-unused-credentials-periksa	AWS Identity and Access Management (IAM) dapat membantu Anda dengan izin akses dan otorisasi dengan memeriksa kata sandi IAM dan kunci akses yang tidak digunakan untuk jangka waktu tertentu. Jika kredensil yang tidak digunakan ini diidentif ikasi, Anda harus menonakti fkan dan/atau menghapus kredensialnya, karena hal ini dapat melanggar prinsip hak istimewa paling sedikit. Aturan ini mengharuskan Anda untuk menetapkan nilai ke maxCredentialUsage Usia (Config Default: 90). Nilai aktual harus mencerminkan kebijakan organisasi Anda.
5.4	secretsmanager-rotation-enabled-check	Aturan ini memastikan AWS rahasia Secrets Manager telah diaktifkan rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotens i mengurangi dampak bisnis jika rahasia itu dikomprom ikan.

ID Kontrol	AWS Aturan Config	Bimbingan
5.4	secretsmanager-scheduled-rotation-success-periksa	Aturan ini memastikan bahwa AWS rahasia Secrets Manager telah berhasil diputar sesuai dengan jadwal rotasi. Memutar rahasia pada jadwal reguler dapat mempersingkat periode di mana rahasia aktif, dan berpotensi mengurangi dampak bisnis jika dikompromikan.
5.4	secretsmanager-secret-periodic-rotation	Aturan ini memastikan AWS rahasia Secrets Manager mengaktifkan rotasi periodik. Memutar rahasia pada jadwal reguler dapat mempersingkat periode rahasia aktif, dan berpotensi mengurangi dampak bisnis jika rahasia itu dikompromikan. Nilai default adalah 90 hari.
5.4	secretsmanager-using-cmk	Untuk membantu melindungi data saat istirahat, pastikan enkripsi dengan AWS Key Management Service (AWS KMS) diaktifkan untuk AWS rahasia Secrets Manager. Karena data sensitif dapat ada saat diam di rahasia Secrets Manager, aktifkan enkripsi saat istirahat untuk membantu melindungi data tersebut.

ID Kontrol	AWS Aturan Config	Bimbingan
6.4	ec2- instance-detailed-monitoring-enabled	Aktifkan aturan ini untuk membantu meningkatkan pemantauan instans Amazon Elastic Compute Cloud (Amazon EC2) di EC2 konsol Amazon, yang menampilkan grafik pemantauan dengan periode 1 menit untuk instans.
6.4	cloudwatch-log-group-encrypted	Untuk membantu melindungi data sensitif saat istirahat, pastikan enkripsi diaktifkan untuk Grup CloudWatch Log Amazon Anda.
6.4	cloud-trail-cloud-watch-logs-diaktifkan	Gunakan Amazon CloudWatch untuk mengumpulkan dan mengelola aktivitas peristiwa log secara terpusat. Penyertaan AWS CloudTrail data memberikan detail aktivitas panggilan API di dalam Anda Akun AWS.

ID Kontrol	AWS Aturan Config	Bimbingan
6.4	cloudtrail-diaktifkan	AWS CloudTrail dapat membantu dalam non-penol akan dengan merekam tindakan AWS Managemen t Console dan panggilan API. Anda dapat mengident ifikasi pengguna dan Akun AWS yang disebut AWS layanan, alamat IP sumber tempat panggilan dihasilka n, dan pengaturan waktu panggilan. Detail data yang diambil terlihat dalam Isi AWS CloudTrail Rekam.
6.4	cloud-trail-encryption-enabled	Karena data sensitif mungkin ada dan untuk membantu melindungi data saat istirahat , pastikan enkripsi diaktifkan untuk AWS CloudTrail jejak Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
6.4	cloud-trail-log-file-validasi-diaktifkan	Memanfaatkan validasi file AWS CloudTrail log untuk memeriksa integritas CloudTrail log. Validasi file log membantu menentukan apakah file log diubah atau dihapus atau tidak diubah setelah CloudTrail dikirimkan. Fitur ini dibangun menggunak an algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus, atau memalsukan CloudTrail file log tanpa deteksi.
6.4	ec2-stopped-instance	Aktifkan aturan ini untuk membantu konfigurasi dasar instans Amazon Elastic Compute Cloud (Amazon EC2) dengan memeriksa apakah EC2 instans Amazon telah dihentikan selama lebih dari jumlah hari yang diizinkan , sesuai dengan standar organisasi Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
6.4	vpc-flow-logs-enabled	Log aliran VPC menyediakan catatan terperinci untuk informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di Amazon Virtual Private Cloud (Amazon VPC) Anda. Secara default, catatan log aliran mencakup nilai untuk berbagai komponen aliran IP, termasuk sumber, tujuan, dan protokol.
6.5A	guardduty-enabled-centralized	Amazon GuardDuty dapat membantu memantau dan mendeteksi potensi peristiwa keamanan siber dengan menggunakan umpan intelijen ancaman. Ini termasuk daftar pembelajaran berbahaya IPs dan mesin untuk mengidentifikasi aktivitas tak terduga, tidak sah, dan berbahaya dalam lingkungan AWS Cloud Anda.

ID Kontrol	AWS Aturan Config	Bimbingan
6.5A	Securityhub diaktifkan	AWS Security Hub membantu memantau personel, koneksi, perangkat, dan perangkat lunak yang tidak sah. AWS Security Hub mengumpul kan, mengatur, dan mempriori taskan peringatan keamanan, atau temuan, dari berbagai layanan. AWS Beberapa layanan tersebut adalah Amazon Security Hub, Amazon Inspector, Amazon AWS Macie, Identity and Access Management (IAM) Access Analyzer, dan Firewall Manager, AWS dan solusi Partner. AWS

Templat

Template tersedia di GitHub: Praktik Terbaik Operasional untuk SWIFT CSP.

Praktik Terbaik Keamanan untuk Amazon Elastic Container Service (Amazon ECS)

Paket kesesuaian ini berisi AWS Config aturan berdasarkan Amazon ECS. Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Keamanan untuk Amazon ECS.

Praktik Terbaik Keamanan untuk Amazon Elastic File System (Amazon EFS)

Paket kesesuaian ini berisi AWS Config aturan berdasarkan Amazon EFS. Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Keamanan untuk Amazon EFS.

Praktik Terbaik Keamanan untuk Amazon Elastic Kubernetes Service (Amazon EKS)

Paket kesesuaian ini berisi AWS Config aturan berdasarkan Amazon EKS. Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Keamanan untuk Amazon EKS.

Praktik Terbaik Keamanan untuk Amazon CloudFront

Paket kesesuaian ini berisi AWS Config aturan berdasarkan Amazon. CloudFront Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Keamanan untuk Amazon CloudFront.

Praktik Terbaik Keamanan untuk OpenSearch Layanan Amazon

Paket kesesuaian ini berisi AWS Config aturan berdasarkan Layanan Amazon. OpenSearch Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Keamanan untuk OpenSearch Layanan Amazon.

Praktik Terbaik Keamanan untuk Amazon Redshift

Paket kesesuaian ini berisi AWS Config aturan berdasarkan Amazon Redshift. Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Keamanan untuk Amazon Redshift.

Praktik Terbaik Keamanan untuk Amazon Relational Database Service (Amazon RDS)

Paket kesesuaian ini berisi AWS Config aturan berdasarkan Amazon RDS. Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Keamanan untuk Amazon RDS.

Praktik Terbaik Keamanan untuk AWS Auto Scaling

Paket kesesuaian ini berisi AWS Config aturan berdasarkan. AWS Auto Scaling Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Keamanan untuk AWS Auto Scaling.

Praktik Terbaik Keamanan untuk AWS CloudTrail

Paket kesesuaian ini berisi AWS Config aturan berdasarkan. AWS CloudTrail Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Keamanan untuk AWS CloudTrail.

Praktik Terbaik Keamanan untuk AWS CodeBuild

Paket kesesuaian ini berisi AWS Config aturan berdasarkan. AWS CodeBuild Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Keamanan untuk AWS CodeBuild.

Praktik Terbaik Keamanan untuk Amazon ECR

Paket kesesuaian ini berisi AWS Config aturan berdasarkan Amazon Elastic Container Registry (Amazon ECR) Registry ECR). Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Keamanan untuk Amazon ECR.

Praktik Terbaik Keamanan untuk AWS Lambda

Paket kesesuaian ini berisi AWS Config aturan berdasarkan. AWS Lambda Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Keamanan untuk AWS Lambda.

Praktik Terbaik Keamanan untuk AWS Network Firewall

Paket kesesuaian ini berisi AWS Config aturan berdasarkan. AWS Network Firewall Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Keamanan untuk AWS Network Firewall.

Praktik Terbaik Keamanan untuk Amazon SageMaker AI

Paket kesesuaian ini berisi AWS Config aturan berdasarkan Amazon AI. SageMaker Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Keamanan untuk Amazon SageMaker AI.

Praktik Terbaik Keamanan untuk AWS Secrets Manager

Paket kesesuaian ini berisi AWS Config aturan berdasarkan. AWS Secrets Manager Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Keamanan untuk AWS Secrets Manager.

Praktik Terbaik Keamanan untuk AWS WAF

Paket kesesuaian ini berisi AWS Config aturan berdasarkan. AWS WAF Untuk daftar semua aturan terkelola yang didukung oleh AWS Config, lihat Daftar Aturan AWS Config Terkelola.

Lihat `Parameters` bagian dalam templat berikut untuk nama dan deskripsi parameter yang diperlukan.

Template tersedia di GitHub: Praktik Terbaik Keamanan untuk AWS WAF.

Contoh Template dengan Tindakan Remediasi

Praktik Terbaik Operasional Untuk Amazon DynamoDB dengan Remediasi

Template tersedia di GitHub: Praktik Terbaik Operasional Untuk Amazon DynamoDB dengan Remediasi.

Praktik Terbaik Operasional Untuk Amazon S3 dengan Remediasi

Template tersedia di GitHub: Praktik Terbaik Operasional Untuk Amazon S3 dengan Remediasi.

Untuk informasi selengkapnya tentang struktur templat, lihat Anatomi Template di Panduan AWS CloudFormation Pengguna.

Membuat template untuk Paket Kesesuaian Kustom untuk AWS Config

Paket kesesuaian kustom adalah kumpulan AWS Config aturan dan tindakan remediasi unik yang dapat Anda terapkan bersama di akun dan AWS Wilayah, atau di seluruh organisasi di. AWS Organizations

Untuk membuat paket kesesuaian kustom, ikuti langkah-langkah di bagian Menyesuaikan template berikut untuk membuat file YAMG yang berisi daftar Aturan AWS Config Terkelola atau Aturan AWS Config Kustom yang ingin Anda kerjakan.

Topik

- Terminologi
- Menyesuaikan template

Terminologi

AWS Config Aturan Terkelola adalah aturan standar yang dimiliki oleh AWS Config.

AWS Config Aturan Kustom adalah aturan yang Anda buat dari awal.

Ada dua cara untuk membuat aturan AWS Config khusus: dengan fungsi Lambda (Panduan AWS Lambda Pengembang) dan dengan Guard (Guard GitHub Repository), sebuah bahasa. policy-as-code AWS Config Aturan kustom AWS Lambda yang dibuat dengan disebut Aturan Lambda AWS Config Kustom dan aturan AWS Config kustom yang dibuat dengan Guard disebut Aturan Kebijakan AWS Config Kustom.

Menyesuaikan template

Membuat file YAMAL Anda

Untuk membuat file YAMG, buka editor teks dan simpan file sebagai .yaml.

> **Note**
>
> File Anda akan berisi bagian Parameter dan Sumber Daya.

Parameter

`Parameters`Bagian dalam file YAMAL Anda adalah untuk parameter aturan untuk kumpulan AWS Config aturan yang akan Anda tambahkan nanti di `Resources` bagian. Buat `Parameters` bagian dengan menyalin dan menempelkan blok kode berikut ke dalam file YAMG Anda, sesuaikan sesuai kebutuhan dan ulangi untuk setiap parameter aturan.

```
Parameters:
    NameOfRuleParamNameOfRuleParameter:
        Default: Parameter value
        Type: Type
    ...
```

Sebagai contoh:

```
Parameters:
    IamPasswordPolicyParamMinimumPasswordLength:
        Default: '14'
        Type: String
```

> **Note**
>
> Saat memilih AWS Config Aturan untuk membangun paket kesesuaian kustom Anda, periksa apakah sumber daya yang disediakan dalam akun Anda yang akan dievaluasi untuk Aturan. AWS Config

1. Baris pertama di bagian parameter setelahnya `Parameters:` adalah string gabungan dari +Param *`NameOfRule`* +. *`NameOfRuleParameter`*

   a. Ganti *`NameOfRule`* dengan nama konsisten yang Anda buat untuk aturan. Misalnya, itu bisa IamPasswordPolicyuntuk iam-password-policy aturan.

   b. Ketik `Param`.

   c. Kemudian, ganti *`NameOfRuleParameter`* dengan nama parameter aturan untuk aturan spesifik Anda. Untuk Aturan AWS Config Terkelola, nama parameter aturan terletak di Daftar Aturan AWS Config Terkelola (misalnya, MinimumPasswordLengthadalah nama parameter aturan untuk iam-password-policyaturan). Untuk Aturan AWS Config Kustom, nama parameter aturan adalah nama yang Anda pilih saat Anda membuat aturan.

2. Jika Anda menggunakan Aturan AWS Config Terkelola, temukan AWS Config aturan yang sesuai dalam daftar aturan terkelola sehingga Anda akan mengetahui nilai yang diterima untuk `Default` dan `Type` untuk aturan khusus Anda. Untuk Aturan AWS Config Kustom, gunakan nilai yang Anda pilih saat membuat aturan.

> **Note**
>
> Untuk setiap parameter, `Type` harus ditentukan. `Type`dapat berupa salah satu dari “String”, “int”, “double”, “CSV”, “boolean” dan "StringMap”.

Sumber Daya

`Resources`Bagian ini mencantumkan aturan yang ditambahkan ke Paket Kesesuaian Kustom Anda. Tambahkan `Resources` blok berikut langsung di bawah `Parameters` bagian Anda, sesuaikan sesuai kebutuhan dan ulangi untuk setiap aturan. Untuk informasi lebih lanjut tentang spesifikasi, lihat AWS::Config::ConfigRule.

```
Resources:
     NameOfRule:
        Properties:
            ConfigRuleName: ActualConfigRuleName
            InputParameters:
                NameOfRuleParameter: !Ref NameOfRuleParamNameOfRuleParameter
            Source:
                Owner: Owner
                SourceIdentifier: SOURCE_IDENTIFIER
        Type: AWS::Config::ConfigRule
     ...
```

Sebagai contoh:

```
Resources:
    IamPasswordPolicy:
        Properties:
            ConfigRuleName: iam-password-policy
            InputParameters:
                MinimumPasswordLength: !Ref IamPasswordPolicyParamMinimumPasswordLength
            Source:
                Owner: AWS
                SourceIdentifier: IAM_PASSWORD_POLICY
```

```
        Type: AWS::Config::ConfigRule
```

> **Note**
>
> Saat memilih AWS Config aturan untuk membuat paket kesesuaian kustom, periksa apakah Anda memiliki sumber daya yang akan dievaluasi untuk AWS Config aturan yang disediakan dalam akun Anda. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.

1. Ganti *NameOfRule* dengan nama yang sama yang Anda buat di `Parameters` bagian.
2. Untuk Aturan AWS Config Terkelola, ganti *ActualConfigRuleName* dengan judul halaman aturan yang sesuai pada Daftar Aturan AWS Config Terkelola. Untuk Aturan AWS Config Kustom, gunakan nama Aturan Config yang Anda pilih pada saat pembuatan aturan.
3. Ganti *NameOfRuleParameter* dengan nama yang sama yang Anda gunakan di `Parameters` bagian ini. Setelah titik dua, salin dan tempel string gabungan yang sama `!Ref` *NameOfRule NameOfRuleParameter* dari+Param+yang Anda buat di bagian. `Parameters`
4. Ubah *Owner* ke nilai yang sesuai.

   > **Note**
   >
   > AWS Config Aturan Terkelola
   > Untuk Aturan AWS Config Terkelola, `Owner` nilainya adalah`AWS`.
   > AWS Config Aturan Kustom
   > Untuk aturan AWS Config khusus yang dibuat dengan Guard, `Owner` nilainya adalah`CUSTOM_POLICY`. Untuk aturan AWS Config khusus yang dibuat dengan Lambda, nilainya adalah. `Owner` `CUSTOM_LAMBDA`

5. Ubah *SOURCE_IDENTIFIER* ke nilai yang sesuai.

   > **Note**
   >
   > AWS Config Aturan Terkelola
   > Untuk Aturan AWS Config Terkelola, salin pengenal dengan mengikuti tautan dari aturan yang Anda pilih dari Daftar Aturan AWS Config Terkelola (misalnya, pengidentifikasi sumber untuk aturan tersebut adalah access-keys-rotatedACCESS_KEYS_ROTATED).
   > AWS Config Aturan Kustom

Untuk aturan AWS Config kustom yang dibuat dengan Lambda, `SourceIdentifier` ini adalah Nama Sumber Daya Amazon (ARN) dari AWS Lambda fungsi aturan, seperti. `arn:aws:lambda:us-east-2:123456789012:function:`*`ActualConfigRuleName`* Untuk aturan AWS Config khusus yang dibuat dengan Guard, bidang ini tidak diperlukan.

Secara keseluruhan, paket kesesuaian kustom yang Anda isi akan mulai terlihat mirip dengan berikut ini, yang merupakan contoh menggunakan Aturan AWS Config Terkelola ini: iam-password-policy,, access-keys-rotateddan -check. iam-user-unused-credentials

```
Parameters:
    IamPasswordPolicyParamMinimumPasswordLength:
        Default: '14'
        Type: String
    AccessKeysRotatedParamMaxAccessKeyAge:
        Default: '90'
        Type: String
    IamUserUnusedCredentialsCheckParamMaxCredentialUsageAge:
        Default: '45'
        Type: String
Resources:
    IamPasswordPolicy:
        Properties:
            ConfigRuleName: iam-password-policy
            InputParameters:
                MinimumPasswordLength: !Ref IamPasswordPolicyParamMinimumPasswordLength
            Source:
                Owner: AWS
                SourceIdentifier: IAM_PASSWORD_POLICY
        Type: AWS::Config::ConfigRule
    AccessKeysRotated:
        Properties:
            ConfigRuleName: access-keys-rotated
            InputParameters:
                maxAccessKeyAge: !Ref AccessKeysRotatedParamMaxAccessKeyAge
            Source:
                Owner: AWS
                SourceIdentifier: ACCESS_KEYS_ROTATED
        Type: AWS::Config::ConfigRule
    IamUserUnusedCredentialsCheck:
        Properties:
```

```
            ConfigRuleName: iam-user-unused-credentials-check
            InputParameters:
                maxCredentialUsageAge: !Ref
IamUserUnusedCredentialsCheckParamMaxCredentialUsageAge
            Source:
                Owner: AWS
                SourceIdentifier: IAM_USER_UNUSED_CREDENTIALS_CHECK
        Type: AWS::Config::ConfigRule
```

Menyebarkan Paket Kesesuaian untuk AWS Config

Anda dapat menggunakan AWS Config konsol atau AWS CLI untuk menyebarkan paket kesesuaian Anda.

Deploy Conformance Packs (Console)

Pada halaman paket Kesesuaian, Anda dapat menerapkan paket kesesuaian untuk akun di Wilayah. Anda juga dapat mengedit dan menghapus paket kesesuaian yang diterapkan.

Anda dapat menerapkan paket kesesuaian menggunakan template AWS Config sampel atau template kustom Anda sendiri. Untuk petunjuk tentang cara membuat paket kesesuaian yang dipersonalisasi, lihat Paket Kesesuaian Kustom.

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Arahkan ke halaman Conformance packs dan pilih Deploy conformance pack.
3. Pada halaman Tentukan templat, pilih templat sampel atau gunakan templat yang ada. Untuk informasi selengkapnya, lihat Templat Contoh Paket Kesesuaian.

   - Jika Anda memilih Gunakan template sampel, pilih Sample template dari daftar dropdown template sampel.

     Untuk informasi tentang isi setiap template, lihat Template Contoh Paket Kesesuaian.
   - Jika Anda memilih Template sudah siap, tentukan sumber template. Ini adalah URI Amazon S3, AWS Systems Manager dokumen (dokumen SSM), atau templat yang Anda unggah.

     Jika template Anda lebih dari 50 KB, unggah ke bucket S3 dan pilih lokasi bucket S3 tersebut. Misalnya: s3://*bucketname/prefix*.

> **Important**
>
> Pilih Template siap jika Anda membuat paket kesesuaian file YAMM dari awal berdasarkan Paket Kesesuaian Kustom.

4. Pilih Berikutnya.
5. Pada halaman Tentukan detail paket kesesuaian, masukkan nama untuk paket kesesuaian Anda.

   Nama paket kesesuaian harus berupa nama unik dengan maksimal 256 karakter alfanumerik. Nama dapat berisi tanda hubung tetapi tidak dapat berisi spasi.
6. Opsional: Tambahkan parameter.

   Parameter didefinisikan dalam template Anda dan membantu Anda mengelola dan mengatur sumber daya Anda.
7. Pilih Berikutnya.
8. Pada halaman Tinjau dan terapkan, tinjau semua informasi.

   Anda dapat mengedit detail template dan detail paket kesesuaian dengan memilih Edit.
9. Pilih Menyebarkan paket kesesuaian.

   AWS Config menampilkan paket kesesuaian pada halaman paket kesesuaian dengan status yang sesuai.

   Jika penerapan paket kesesuaian Anda gagal, periksa izin Anda, verifikasi bahwa Anda telah melakukan langkah-langkah prasyarat, dan coba lagi. Atau Anda dapat menghubungi AWS Dukungan.

Untuk menerapkan paket kesesuaian menggunakan template sampel dengan remediasi, lihat A. Prasyarat untuk Menggunakan Paket Kesesuaian Dengan Remediasi dan kemudian gunakan prosedur sebelumnya.

Untuk menerapkan paket kesesuaian dengan satu atau beberapa AWS Config aturan, lihat. B. Prasyarat untuk Menggunakan Paket Kesesuaian Dengan Satu atau Lebih Aturan Kustom AWS Config

Deploy Conformance Packs (AWS CLI)

1. Buka jendela command prompt atau terminal.
2. Masukkan salah satu perintah berikut untuk menyebarkan paket kesesuaian bernama. **`MyConformancePack`** Sumber template adalah URI Amazon S3, template yang Anda unggah, atau AWS Systems Manager dokumen (dokumen SSM).

   Amazon S3 URI

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-s3-uri "s3://amzn-s3-demo-bucket/templateName.yaml"
   --delivery-s3-bucket amzn-s3-demo-bucket
   ```

   Template YAMB dari direktori lokal Anda

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-body template body
   ```

   AWS Systems Manager Dokumen (Dokumen Systems Manager)

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-ssm-document-details
    DocumentName=SSMDocumentName,DocumentVersion=SSMDocumentVersion
   --delivery-s3-bucket amzn-s3-demo-bucket
   ```

3. Tekan Enter untuk menjalankan perintah.

   Anda akan melihat output seperti yang berikut ini.

   ```
   {
       "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/
   MyConformancePack1/conformance-pack-ID"
   }
   ```

> **Note**
>
> Untuk informasi selengkapnya tentang membuat template YAMB untuk paket kesesuaian, lihat Paket Kesesuaian Kustom.

Mengedit Paket Kesesuaian untuk AWS Config

Anda dapat menggunakan AWS Config konsol atau AWS CLI untuk mengedit paket kesesuaian Anda.

Editing Conformance Packs (Console)

1. Untuk mengedit paket kesesuaian, pilih paket kesesuaian dari tabel.
2. Pilih Tindakan dan kemudian pilih Edit.
3. Pada halaman Edit paket kesesuaian, Anda dapat mengedit detail templat, templat sampel, paket kesesuaian, dan bagian parameter.

   Anda tidak dapat mengubah nama paket kesesuaian.
4. Pilih Simpan perubahan.

   Paket kesesuaian ditampilkan dengan aturan. AWS Config

Editing Conformance Packs (AWS CLI)

Jika Anda mengedit paket kesesuaian yang Anda tambahkan sebelumnya, gunakan `PutConformancePack` perintah yang sama yang Anda gunakan saat menerapkan paket kesesuaian.

1. Buka jendela command prompt atau terminal.
2. Masukkan salah satu perintah berikut untuk menyebarkan paket kesesuaian bernama. **`MyConformancePack`** Sumber template adalah URI Amazon S3, template yang Anda unggah, atau AWS Systems Manager dokumen (dokumen SSM).

   Amazon S3 URI

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   ```

```
--template-s3-uri "s3://amzn-s3-demo-bucket/templateName.yaml"
--delivery-s3-bucket amzn-s3-demo-bucket
```

Template YAMM dari direktori lokal Anda

```
aws configservice put-conformance-pack
--conformance-pack-name MyConformancePack
--template-body template body
```

AWS Systems Manager Dokumen (Dokumen Systems Manager)

```
aws configservice put-conformance-pack
--conformance-pack-name MyConformancePack
--template-ssm-document-details
 DocumentName=SSMDocumentName,DocumentVersion=SSMDocumentVersion
--delivery-s3-bucket amzn-s3-demo-bucket
```

3. Tekan Enter untuk menjalankan perintah.

   Anda akan melihat output seperti yang berikut ini.

```
{
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/
MyConformancePack1/conformance-pack-ID"
}
```

> **Note**
>
> Untuk informasi selengkapnya tentang membuat template YAMAL untuk paket kesesuaian, lihat Paket Kesesuaian Kustom.

Menghapus Paket Kesesuaian untuk AWS Config

Anda dapat menggunakan AWS Config konsol atau AWS CLI untuk menghapus paket kesesuaian.

Pertimbangan

Rekomendasi: Pertimbangkan untuk mengecualikan jenis **`AWS::Config::ResourceCompliance`** sumber daya dari rekaman sebelum menghapus aturan

Menghapus aturan membuat item konfigurasi (CIs) untuk `AWS::Config::ResourceCompliance` itu dapat memengaruhi biaya Anda untuk perekam konfigurasi. Jika Anda menghapus aturan yang mengevaluasi sejumlah besar jenis sumber daya, ini dapat menyebabkan lonjakan jumlah CIs yang direkam.

Untuk menghindari biaya terkait, Anda dapat memilih untuk menonaktifkan perekaman untuk jenis `AWS::Config::ResourceCompliance` sumber daya sebelum menghapus aturan, dan mengaktifkan kembali perekaman setelah aturan dihapus.

Namun, karena menghapus aturan adalah proses asinkron, mungkin perlu satu jam atau lebih untuk menyelesaikannya. Selama perekaman dinonaktifkan`AWS::Config::ResourceCompliance`, evaluasi aturan tidak akan dicatat dalam riwayat sumber daya terkait.

Untuk menghapus paket kesesuaian

Deleting Conformance Packs (Console)

1. Untuk menghapus paket kesesuaian, pilih paket kesesuaian dari tabel.
2. Pilih Tindakan dan kemudian pilih Hapus.
3. Pada kotak *`conformance pack`* dialog hapus, konfirmasikan apakah Anda ingin menghapus paket kesesuaian ini secara permanen.

   > **Important**
   >
   > Anda tidak dapat mengembalikan tindakan ini. Saat menghapus paket kesesuaian, Anda menghapus semua AWS Config aturan dan tindakan remediasi dalam paket kesesuaian tersebut.

4. Masukkan Hapus dan pilih Hapus.

   Pada halaman paket Kesesuaian, Anda dapat melihat status penerapan sebagai Menghapus hingga paket kesesuaian dihapus sepenuhnya.

Deleting Conformance Packs (AWS CLI)

Masukkan perintah berikut.

```
aws configservice delete-conformance-pack --conformance-pack-name MyConformancePack1
```

Jika berhasil, perintah berjalan tanpa output tambahan.

> **Important**
>
> Anda tidak dapat mengembalikan tindakan ini. Saat menghapus paket kesesuaian, Anda menghapus semua AWS Config aturan dan tindakan remediasi dalam paket kesesuaian tersebut.

Melihat Detail dan Informasi Kepatuhan untuk Paket Kesesuaian Anda AWS Config

> **Important**
>
> Untuk pelaporan yang akurat tentang status kepatuhan, Anda harus mencatat jenis `AWS::Config::ResourceCompliance` sumber daya. Untuk informasi selengkapnya, lihat Merekam AWS Sumber Daya.

Anda dapat menggunakan AWS Config konsol atau AWS CLI untuk melihat paket kesesuaian Anda. AWS Config Konsol memiliki dasbor terpadu. AWS CLI Ini memungkinkan Anda menjalankan perintah untuk informasi tertentu.

Viewing Conformance Packs (Console)

Untuk melihat paket kesesuaian Anda di AWS Management Console, lihat Paket Dasbor Paket Kesesuaian.

Viewing the Details for your Conformance Packs (AWS CLI)

1. Masukkan perintah berikut.

   ```
   aws configservice describe-conformance-packs
   ```

ATAU

```
aws configservice describe-conformance-packs --conformance-pack-
name="MyConformancePack1"
```

2. Anda akan melihat output seperti yang berikut ini.

```
{
    "conformancePackName": "MyConformancePack1",
    "conformancePackId": "conformance-pack-ID",
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-
pack/MyConformancePack1/conformance-pack-ID",
    "conformancePackInputParameters": [],
    "lastUpdateRequestedTime": "Thu Jul 18 16:07:05 PDT 2019"
}
```

Viewing the Status for your Conformance Packs (AWS CLI)

1. Masukkan perintah berikut.

```
aws configservice describe-conformance-pack-status --conformance-pack-
name="MyConformancePack1"
```

2. Anda akan melihat output seperti yang berikut ini.

```
{
    "stackArn": "arn:aws:cloudformation:us-west-2:AccountID:stack/
awsconfigconforms-MyConformancePack1-conformance-pack-ID/d4301fe0-
a9b1-11e9-994d-025f28dd83ba",
    "conformancePackName": "MyConformancePack1",
    "conformancePackId": "conformance-pack-ID",
    "lastUpdateCompletedTime": "Thu Jul 18 16:15:17 PDT 2019",
    "conformancePackState": "CREATE_COMPLETE",
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-
pack/MyConformancePack1/conformance-pack-ID",
    "lastUpdateRequestedTime": "Thu Jul 18 16:14:35 PDT 2019"
}
```

Viewing the Compliance Status for your Conformance Packs (AWS CLI)

1. Masukkan perintah berikut.

```
aws configservice describe-conformance-pack-compliance --conformance-pack-
name="MyConformancePack1"
```

2. Anda akan melihat output seperti yang berikut ini.

```
{
    "conformancePackName": "MyConformancePack1",
    "conformancePackRuleComplianceList": [
        {
            "configRuleName": "awsconfigconforms-RuleName1-conformance-pack-ID",
            "complianceType": "NON_COMPLIANT"
        },
        {
            "configRuleName": "awsconfigconforms-RuleName2-conformance-pack-ID",
            "complianceType": "COMPLIANT"
        }
    ]
}
```

Viewing the Compliance Details for your Conformance Packs (AWS CLI)

1. Masukkan perintah berikut.

```
aws configservice get-conformance-pack-compliance-details --conformance-pack-
name="MyConformancePack1"
```

2. Anda semestinya melihat output yang serupa berikut.

```
{
    "conformancePackRuleEvaluationResults": [
        {
            "evaluationResultIdentifier": {
                "orderingTimestamp": "Tue Jul 16 23:07:35 PDT 2019",
                "evaluationResultQualifier": {
                    "resourceId": "resourceID",
                    "configRuleName": "awsconfigconforms-RuleName1-conformance-
pack-ID",
```

```
                    "resourceType": "AWS::::Account"
                }
            },
            "configRuleInvokedTime": "Tue Jul 16 23:07:50 PDT 2019",
            "resultRecordedTime": "Tue Jul 16 23:07:51 PDT 2019",
            "complianceType": "NON_COMPLIANT"
        },
        {
            "evaluationResultIdentifier": {
                "orderingTimestamp": "Thu Jun 27 15:16:36 PDT 2019",
                "evaluationResultQualifier": {
                    "resourceId": "resourceID",
                    "configRuleName": "awsconfigconforms-RuleName2-conformance-
pack-ID",
                    "resourceType": "AWS::EC2::SecurityGroup"
                }
            },
           "configRuleInvokedTime": "Thu Jul 11 23:08:06 PDT 2019",
            "resultRecordedTime": "Thu Jul 11 23:08:06 PDT 2019",
            "complianceType": "COMPLIANT"
        }
    ],
    "conformancePackName": "MyConformancePack1"
}
}
```

Melihat Timeline Riwayat Kepatuhan untuk Paket Kesesuaian untuk AWS Config

AWS Config mendukung penyimpanan perubahan status kepatuhan ke paket kesesuaian Anda. Ini memungkinkan Anda untuk melihat riwayat perubahan status kepatuhan. Perubahan status kepatuhan ini disajikan sebagai garis waktu. Garis waktu menangkap perubahan `ConfigurationItems` selama periode waktu tertentu. Anda juga dapat menggunakan fitur ini untuk menemukan aturan tertentu dalam paket kesesuaian yang tidak sesuai.

Anda dapat memilih masuk atau keluar untuk merekam semua jenis sumber daya AWS Config. Jika Anda memilih untuk merekam semua jenis sumber daya, AWS Config secara otomatis mulai merekam riwayat kepatuhan paket kesesuaian seperti yang dievaluasi oleh Aturan. AWS Config Secara default, AWS Config mencatat perubahan konfigurasi untuk semua sumber daya yang didukung. Anda juga dapat memilih hanya jenis sumber daya riwayat kepatuhan paket

kesesuaian tertentu:. `AWS::Config::ConformancePackCompliance` Rekaman untuk jenis `AWS::Config::ConformancePackCompliance` sumber daya tersedia tanpa biaya tambahan. Untuk informasi selengkapnya, lihat Merekam AWS Sumber Daya.

Paket kesesuaian sesuai jika semua aturan dalam paket kesesuaian sesuai. Tidak patuh jika ada aturan yang tidak sesuai. Status kepatuhan paket kesesuaian adalah INSUFFICIENT_DATA hanya jika semua aturan dalam paket kesesuaian tidak dapat dievaluasi karena data yang tidak mencukupi. Jika beberapa aturan dalam paket kesesuaian sesuai tetapi status kepatuhan aturan lain dalam paket kesesuaian yang sama adalah INSUFFICIENT_DATA, paket kesesuaian menunjukkan kepatuhan. Kepatuhan untuk paket kesesuaian tidak dievaluasi sekaligus. Beberapa aturan mungkin membutuhkan waktu lebih lama untuk dievaluasi daripada yang lain. Kepatuhan dievaluasi untuk kelompok aturan pada satu waktu, berlanjut secara bertahap sampai semua aturan dalam paket kesesuaian telah dievaluasi.

Melihat Timeline Kepatuhan

Akses timeline kepatuhan dengan memilih paket kesesuaian tertentu dari halaman utama paket Kesesuaian.

1. Arahkan ke halaman Paket Kesesuaian.
2. Pada halaman utama Conformance Pack, pilih paket kesesuaian tertentu dan kemudian pilih timeline paket Conformance.

> **Note**
>
> Atau, Anda dapat menggunakan timeline kepatuhan dari halaman detail paket kesesuaian. Pilih paket kesesuaian dan pilih Lihat detail di dropdown Tindakan. Dari halaman ini, pilih Timeline paket Kesesuaian.

Garis waktu menunjukkan riwayat perubahan status kepatuhan untuk paket kesesuaian. Anda dapat melakukan tindakan berikut:

1. Perluas perubahan kepatuhan untuk melihat status line-by-line kepatuhan setiap aturan dalam paket kesesuaian.
2. Dari tampilan yang diperluas, pilih aturan tertentu untuk melihat halaman detailnya.

Menanyakan Riwayat Kepatuhan untuk Paket Kesesuaian untuk AWS Config

Kueri riwayat kepatuhan menggunakan get-resource-config-history menggunakan jenis sumber dayaAWS::Config::ConformancePackCompliance.

```
aws configservice get-resource-config-history --resource-type
 AWS::Config::ConformancePackCompliance --resource-id conformance-pack-ID
```

Anda akan melihat output yang serupa dengan yang berikut:

```
{
    "configurationItems": [
        {
            "version": "1.3",
            "accountId": "Account ID",
            "configurationItemCaptureTime": 1614641951.442,
            "configurationItemStatus": "OK",
            "configurationStateId": "1614641951442",
            "configurationItemMD5Hash": "",
            "arn": "arn:aws:config:us-east-1:Account ID:conformance-
pack/MyConformancePack1/conformance-pack-ID",
            "resourceType": "AWS::Config::ConformancePackCompliance",
            "resourceId": "conformance-pack-ID",
            "resourceName": "MyConformancePack1",
            "awsRegion": "us-east-1",
            "tags": {},
            "relatedEvents": [],
            "relationships": [],
            "configuration": "{\"compliantRuleCount\":1,\"configRuleList\":
[{\"configRuleName\":\"RuleName1-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-nnnnnn\",\"complianceType\":\"INSUFFICIENT_DATA\"},
{\"configRuleName\":\"RuleName2-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-mmmmmm\",\"complianceType\":\"COMPLIANT\"},
{\"configRuleName\":\"RuleName3-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-pppppp\",\"complianceType\":\"INSUFFICIENT_DATA\"}],
\"totalRuleCount\":3,\"nonCompliantRuleCount\":0,\"complianceType\":\"COMPLIANT\"}",
            "supplementaryConfiguration": {}
        },
```

```
        {
            "version": "1.3",
            "accountId": "768311917693",
            "configurationItemCaptureTime": 1605551029.515,
            "configurationItemStatus": "ResourceDiscovered",
            "configurationStateId": "1605551029515",
            "configurationItemMD5Hash": "",
            "resourceType": "AWS::Config::ConformancePackCompliance",
            "resourceId": "conformance-pack-ID",
            "resourceName": "MyConformancePack1",
            "awsRegion": "us-east-1",
            "tags": {},
            "relatedEvents": [],
            "relationships": [],
            "configuration": "{\"compliantRuleCount\":1,\"configRuleList\":
[{\"configRuleName\":\"RuleName1-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-nnnnnn\",\"complianceType\":\"INSUFFICIENT_DATA\"},
{\"configRuleName\":\"RuleName2-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-mmmmmm\",\"complianceType\":\"COMPLIANT\"},
{\"configRuleName\":\"RuleName3-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-pppppp\",\"complianceType\":\"INSUFFICIENT_DATA\"}],
\"totalRuleCount\":3,\"nonCompliantRuleCount\":0,\"complianceType\":\"COMPLIANT\"}",
            "supplementaryConfiguration": {}
        }
    ]
}
```

Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung (AWS Config) dan GetResourceConfigHistorydalam referensi API.

Mengelola Paket Kesesuaian untuk Semua Akun AWS Config di Organisasi Anda

Gunakan AWS Config untuk mengelola paket kesesuaian di semua Akun AWS dalam organisasi. Anda dapat melakukan tindakan berikut:

- Terapkan, perbarui, dan hapus paket kesesuaian secara terpusat di seluruh akun anggota dalam organisasi di. AWS Organizations

- Terapkan seperangkat AWS Config aturan dan tindakan remediasi umum di semua akun dan tentukan akun di mana AWS Config aturan dan tindakan remediasi tidak boleh dibuat.
- Gunakan akun manajemen AWS Organizations untuk menegakkan tata kelola dengan memastikan bahwa AWS Config aturan dan tindakan remediasi yang mendasari tidak dapat dimodifikasi oleh akun anggota organisasi Anda.

Pertimbangan

Untuk penyebaran di berbagai wilayah

Panggilan API untuk menerapkan aturan dan paket kesesuaian di seluruh akun adalah spesifik Wilayah. AWS Di tingkat organisasi, Anda perlu mengubah konteks panggilan API ke wilayah lain jika ingin menerapkan aturan di wilayah lain. Misalnya, untuk menerapkan aturan di AS Timur (Virginia N.), ubah wilayah ke AS Timur (Virginia N.) dan kemudian hubungi. `PutOrganizationConfigRule`

Untuk akun dalam suatu organisasi

Jika akun baru bergabung dengan organisasi, aturan atau paket kesesuaian diterapkan ke akun tersebut. Ketika akun meninggalkan organisasi, aturan atau paket kesesuaian dihapus.

Jika Anda menerapkan aturan organisasi atau paket kesesuaian di akun administrator organisasi, lalu membuat administrator yang didelegasikan dan menerapkan aturan organisasi atau paket kesesuaian di akun administrator yang didelegasikan, Anda tidak akan dapat melihat aturan organisasi atau paket kesesuaian di akun administrator organisasi dari akun administrator yang didelegasikan atau melihat aturan organisasi atau paket kesesuaian dalam akun administrator yang didelegasikan dari akun administrator organisasi. The DescribeOrganizationConfigRulesdan hanya DescribeOrganizationConformancePacks APIs dapat melihat dan berinteraksi dengan sumber daya terkait organisasi yang digunakan dari dalam akun yang memanggilnya. APIs

Coba lagi mekanisme untuk akun baru yang ditambahkan ke organisasi

Penerapan aturan organisasi yang ada dan paket kesesuaian hanya akan dicoba ulang selama 7 jam setelah akun ditambahkan ke organisasi Anda jika perekam tidak tersedia. Anda diharapkan untuk membuat perekam jika tidak ada dalam waktu 7 jam setelah menambahkan akun ke organisasi Anda.

Akun manajemen organisasi, administrator yang didelegasikan, dan peran terkait layanan

Jika Anda menggunakan akun manajemen organisasi dan ingin menggunakan administrator yang didelegasikan untuk penerapan organisasi, ketahuilah bahwa tidak AWS Config akan secara otomatis

membuat peran terkait layanan (SLR). Anda harus secara manual membuat peran terkait layanan (SLR) secara terpisah menggunakan IAM.

Jika Anda tidak memiliki SLR untuk akun manajemen Anda, Anda tidak akan dapat menyebarkan sumber daya ke akun itu dari akun administrator yang didelegasikan. Anda masih dapat menerapkan paket kesesuaian ke akun anggota dari akun manajemen dan administrator yang didelegasikan. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan di Panduan Pengguna AWS Identity and Access Management (IAM).

Deployment

To deploy with the AWS Management Console

Untuk menerapkan paket kesesuaian di seluruh organisasi dari konsol, gunakan. AWS AWS Systems ManagerUntuk informasi selengkapnya, lihat Menerapkan paket AWS Config kesesuaian di Panduan Pengguna.AWS Systems Manager

To deploy with the AWS API

Untuk informasi tentang cara mengintegrasikan AWS Config dengan AWS Organizations, lihat AWS Config dan AWS Organizations di Panduan AWS Organizations Pengguna. Pastikan AWS Config perekaman aktif sebelum Anda menggunakan yang berikut ini APIs untuk mengelola aturan paket kesesuaian di semua Akun AWS dalam organisasi:

- DeleteOrganizationConformancePack, menghapus paket kesesuaian organisasi yang ditentukan dan semua aturan konfigurasi dan tindakan remediasi dari semua akun anggota di organisasi itu.
- DescribeOrganizationConformancePacks, mengembalikan daftar paket kesesuaian organisasi.
- DescribeOrganizationConformancePackStatuses, menyediakan status penyebaran paket kesesuaian organisasi untuk organisasi.
- GetOrganizationConformancePackDetailedStatus, mengembalikan status terperinci untuk setiap akun anggota dalam organisasi untuk paket kesesuaian organisasi tertentu.
- PutOrganizationConformancePack, menyebarkan paket kesesuaian di seluruh akun anggota dalam Organisasi. AWS

Support Wilayah

Menerapkan paket kesesuaian di seluruh akun anggota di AWS Organisasi didukung di Wilayah berikut.

Nama Wilayah	Wilayah	Titik Akhir	Protokol
AS Timur (Ohio)	us–east-2	config.us-east-2.amazonaws.com	HTTPS
AS Timur (Virginia Utara)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
AS Barat (California Utara)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
AS Barat (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
Afrika (Cape Town)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asia Pasifik (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asia Pasifik (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asia Pasifik (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Asia Pasifik (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia Pasifik (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pasifik (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia Pasifik (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia Pasifik (Singapura)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pasifik (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Kanada (Pusat)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Kanada Barat (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Eropa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Eropa (Irlandia)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Eropa (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Eropa (Milan)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Eropa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Eropa (Spanyol)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Eropa (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Eropa (Zürich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Timur Tengah (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Timur Tengah (UAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Amerika Selatan (Sao Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (AS-Timur)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (AS-Barat)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Pemecahan Masalah untuk Paket Kesesuaian untuk AWS Config

Periksa masalah berikut untuk membantu memecahkan masalah yang mungkin Anda hadapi saat menggunakan paket kesesuaian.

Topik

- Status gagal untuk paket kesesuaian
- Aturan menggantung dalam paket kesesuaian

Status gagal untuk paket kesesuaian

Jika Anda mendapatkan kesalahan yang menunjukkan bahwa paket kesesuaian gagal saat membuat, memperbarui, atau menghapusnya, Anda dapat memeriksa status paket kesesuaian Anda.

```
aws configservice describe-conformance-pack-status --conformance-pack-name
 MyConformancePack1
```

Anda akan melihat output seperti yang berikut ini.

```
"ConformancePackStatusDetails": [
    {
        "ConformancePackName": "ConformancePackName",
        "ConformancePackId": "ConformancePackId",
        "ConformancePackArn": "ConformancePackArn",
        "ConformancePackState": "CREATE_FAILED",
        "StackArn": "CloudFormation stackArn",
        "ConformancePackStatusReason": "Failure Reason",
        "LastUpdateRequestedTime": 1573865201.619,
        "LastUpdateCompletedTime": 1573864244.653
    }
]
```

Periksa ConformancePackStatusReasoninformasi tentang kegagalan.

Ketika StackArn hadir dalam respons

Jika pesan kesalahan tidak jelas atau jika kegagalan disebabkan oleh kesalahan internal, buka AWS CloudFormation konsol dan lakukan hal berikut:

1. Cari StackArn dari output.
2. Pilih tab Peristiwa CloudFormation tumpukan dan periksa peristiwa yang gagal.

   Alasan status menunjukkan mengapa paket kesesuaian gagal.

Ketika StackArn tidak ada dalam respons

Jika Anda menerima kegagalan saat membuat paket kesesuaian tetapi StackArn tidak ada dalam respons status, alasan yang mungkin adalah pembuatan tumpukan gagal dan memutar kembali dan menghapus tumpukan. CloudFormation Buka CloudFormation konsol dan cari tumpukan yang berada dalam keadaan Dihapus. Tumpukan yang gagal mungkin tersedia di sana. CloudFormation Tumpukan berisi nama paket kesesuaian. Jika Anda menemukan tumpukan yang gagal, pilih tab Peristiwa CloudFormation tumpukan dan periksa peristiwa yang gagal.

Jika tidak satu pun dari langkah-langkah ini berhasil dan jika alasan kegagalan adalah kesalahan layanan internal, maka coba operasi lagi atau hubungi AWS Dukungan Pusat.

Aturan menggantung dalam paket kesesuaian

Menyebarkan paket kesesuaian melibatkan pembuatan AWS CloudFormation tumpukan yang mendasari di latar belakang untuk menerapkan aturan dalam template paket kesesuaian. Aturan ini adalah aturan terkait layanan dan tidak dapat diperbarui atau dihapus di luar paket kesesuaian.

Jika Anda membuat perubahan pada CloudFormation tumpukan yang mendasarinya, ini menghasilkan situasi di mana paket kesesuaian dan aturannya menjadi tidak dapat dikelola. Aturan yang tidak dapat dikelola ini adalah aturan yang menggantung.

Melayang di antara CloudFormation tumpukan dan paket kesesuaian

Anda dapat memperbarui nama aturan dalam template paket kesesuaian langsung dari konsol. CloudFormation Jika Anda memperbarui template langsung dari CloudFormation konsol, ini tidak memperbarui paket kesesuaian yang diterapkan.

Penyimpangan ini menciptakan aturan menggantung. Jika Anda mencoba menghapus aturan dari paket kesesuaian, Anda menerima kesalahan yang mirip dengan berikut ini:

```
"An AWS service owns ServiceLinkedConfigRule. You do not have permissions to
 take action on this rule. (Service: AmazonConfig; Status Code: 400; Error Code:
 AccessDeniedException; Request ID: my-request-ID; Proxy: null)".
```

Jika Anda mencoba menghapus paket kesesuaian, aturan menggantung tidak dapat dihapus dan Anda menerima kesalahan yang mirip dengan berikut ini:

```
"User: arn:aws:sts::111122223333:assumed-role/AWSServiceRoleForConfigConforms/
AwsConfigConformsWorkflow is not authorized to perform: config:DeleteConfigRule on
 resource: my-dangling-rule
```

Untuk memperbaiki masalah ini, lakukan langkah-langkah berikut:

1. Hapus tumpukan. Untuk informasi selengkapnya, lihat Menghapus tumpukan di AWS CloudFormation konsol di Panduan CloudFormation Pengguna.
2. Hapus paket kesesuaian menggunakan AWS Config konsol atau menggunakan API. DeleteConformancePack Jika ini adalah paket kesesuaian organisasi dan Anda menggunakan manajemen atau akun administrator yang didelegasikan, gunakan API. DeleteOrganizationConformancePack

3. Hubungi AWS Dukungan Pusat dengan Nama Sumber Daya Amazon (ARN) dari aturan menggantung dalam paket kesesuaian untuk membantu membersihkan akun Anda.

Untuk menghindari masalah ini, ingat praktik terbaik ini:

- Jangan pernah melakukan pembaruan langsung ke CloudFormation tumpukan paket kesesuaian.
- Jangan pernah mencoba dan membuat perubahan yang membuat penyimpangan antara paket kesesuaian dan tumpukan dasarnya. CloudFormation
- Service-linked role (SLR) untuk paket kesesuaian tidak dapat dimodifikasi. Pastikan sumber daya yang Anda perbarui adalah bagian dari kebijakan izin untuk SLR.

CloudFormation Tumpukan yang dihapus untuk paket kesesuaian

Kecuali ada penyimpangan antara CloudFormation tumpukan dan paket kesesuaian, tidak pernah disarankan untuk menghapus aturan dalam paket kesesuaian atau tumpukannya langsung dari konsol. CloudFormation CloudFormation

Untuk memperbaiki masalah ini, hubungi AWS Dukungan Pusat dengan Nama Sumber Daya Amazon (ARN) dari aturan yang menggantung dalam paket kesesuaian untuk membantu membersihkan akun Anda.

Untuk menghindari masalah ini, ingat praktik terbaik ini:

- Jangan pernah menghapus CloudFormation tumpukan yang mendasarinya untuk paket kesesuaian.
- Hapus paket kesesuaian menggunakan API. DeleteConformancePack Jika ini adalah paket kesesuaian organisasi dan Anda menggunakan manajemen atau akun administrator yang didelegasikan, gunakan API. DeleteOrganizationConformancePack

Memulihkan Sumber Daya yang Tidak Sesuai dengan AWS Config

AWS Config memungkinkan Anda untuk memulihkan sumber daya yang tidak patuh yang dievaluasi oleh. Aturan AWS Config AWS Config menerapkan remediasi menggunakan dokumen AWS Systems Manager Otomasi. Dokumen-dokumen ini menentukan tindakan yang akan dilakukan pada AWS sumber daya yang tidak patuh yang dievaluasi oleh. Aturan AWS Config Anda dapat mengaitkan dokumen SSM dengan menggunakan AWS Management Console atau menggunakan APIs.

AWS Config menyediakan satu set dokumen otomatisasi terkelola dengan tindakan remediasi. Anda juga dapat membuat dan mengaitkan dokumen otomatisasi khusus dengan AWS Config aturan.

Topik

- Support Wilayah
- Menyiapkan Remediasi Manual untuk AWS Config
- Menyiapkan Remediasi Otomatis untuk AWS Config
- Menghapus Tindakan Remediasi untuk AWS Config

Support Wilayah

Saat ini, tindakan remediasi untuk AWS Config Aturan didukung di wilayah berikut:

Nama Wilayah	Wilayah	Titik Akhir	Protokol
AS Timur (Ohio)	us–east-2	config.us-east-2.amazonaws.com	HTTPS
AS Timur (Virginia Utara)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
AS Barat (Californ ia Utara)	us-west-1	config.us-west-1.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
AS Barat (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
Afrika (Cape Town)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asia Pasifik (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asia Pasifik (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asia Pasifik (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asia Pasifik (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia Pasifik (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pasifik (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Asia Pasifik (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia Pasifik (Singapura)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pasifik (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pasifik (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Kanada (Pusat)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Kanada Barat (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Eropa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Eropa (Irlandia)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Eropa (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Eropa (Milan)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Eropa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Eropa (Spanyol)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Eropa (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Eropa (Zürich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Timur Tengah (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Timur Tengah (UAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
Amerika Selatan (Sao Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (AS-Timur)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol	
AWS GovCloud (AS-Barat)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS	

Menyiapkan Remediasi Manual untuk AWS Config

Untuk menerapkan remediasi pada sumber daya yang tidak sesuai, Anda dapat memilih tindakan remediasi yang ingin Anda kaitkan dari daftar yang telah diisi sebelumnya atau membuat tindakan remediasi kustom Anda sendiri menggunakan dokumen SSM. AWS Config memberikan daftar tindakan remediasi yang direkomendasikan di. AWS Management Console

Setting Up Manual Remediation (Console)

Di dalam AWS Management Console, Anda dapat memilih untuk memulihkan sumber daya yang tidak sesuai secara manual dengan mengaitkan tindakan remediasi dengan aturan. AWS Config Dengan semua tindakan remediasi, Anda dapat memilih remediasi manual atau otomatis.

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Pilih Aturan di sebelah kiri dan kemudian pada halaman Aturan, pilih Tambahkan Aturan untuk menambahkan aturan baru ke daftar aturan

   Untuk aturan yang ada, pilih aturan yang tidak sesuai dari daftar aturan dan pilih daftar dropdown Tindakan.
3. Dari daftar dropdown Tindakan, pilih Kelola remediasi. Pilih “Remediasi manual” dan kemudian pilih tindakan remediasi yang sesuai dari daftar yang direkomendasikan.

> **Note**
>
> Anda hanya dapat mengelola remediasi untuk aturan terkait AWS Config non-layanan. Untuk informasi selengkapnya, lihat Aturan Tertaut Layanan AWS.

Bergantung pada tindakan remediasi yang dipilih, Anda melihat parameter tertentu atau tidak ada parameter.

4. (Opsional): Jika Anda ingin meneruskan ID sumber daya sumber daya yang tidak sesuai ke tindakan remediasi, pilih parameter ID Sumber Daya. Jika dipilih, saat runtime parameter tersebut diganti dengan ID sumber daya yang akan diperbaiki.

   Setiap parameter memiliki nilai statis atau nilai dinamis. Jika Anda tidak memilih parameter ID sumber daya tertentu dari daftar dropdown, Anda dapat memasukkan nilai untuk setiap tombol. Jika Anda memilih parameter ID sumber daya dari daftar dropdown, Anda dapat memasukkan nilai untuk semua kunci lainnya kecuali parameter ID sumber daya yang dipilih.

5. Pilih Simpan. Halaman Aturan ditampilkan.

Untuk mengatasi masalah tindakan remediasi yang gagal, Anda dapat menjalankan AWS perintah Command Line Interface `describe-remediation-execution-status` untuk mendapatkan tampilan rinci Eksekusi Remediasi untuk sekumpulan sumber daya. Detailnya mencakup status, stempel waktu untuk langkah-langkah eksekusi remediasi, dan pesan kesalahan apa pun untuk langkah-langkah yang gagal.

Setting Up Manual Remediation (API)

Gunakan operasi AWS Config API berikut untuk menyiapkan remediasi manual:

- PutRemediationConfigurations, menambahkan atau memperbarui konfigurasi remediasi dengan AWS Config aturan tertentu dengan target atau tindakan yang dipilih.
- StartRemediationExecution, menjalankan remediasi sesuai permintaan untuk AWS Config aturan yang ditentukan terhadap konfigurasi remediasi terakhir yang diketahui.
- DescribeRemediationExecutionStatus, memberikan tampilan terperinci tentang Eksekusi Remediasi untuk sekumpulan sumber daya termasuk status, stempel waktu kapan langkah-langkah untuk eksekusi remediasi terjadi, dan pesan kesalahan apa pun untuk langkah-langkah yang gagal.
- DescribeRemediationConfigurations, mengembalikan rincian dari satu atau lebih konfigurasi remediasi.

Menyiapkan Remediasi Otomatis untuk AWS Config

Untuk menerapkan remediasi pada sumber daya yang tidak sesuai, Anda dapat memilih tindakan remediasi yang ingin Anda kaitkan dari daftar yang telah diisi sebelumnya atau membuat tindakan remediasi kustom Anda sendiri menggunakan dokumen SSM. AWS Config memberikan daftar tindakan remediasi di. AWS Management Console

Setting Up Auto Remediation (Console)

Di dalam AWS Management Console, Anda dapat memilih untuk secara otomatis memulihkan sumber daya yang tidak sesuai dengan mengaitkan tindakan remediasi dengan aturan. AWS Config Dengan semua tindakan remediasi, Anda dapat memilih remediasi manual atau otomatis.

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Pilih Aturan di sebelah kiri dan kemudian pada halaman Aturan, pilih Tambahkan Aturan untuk menambahkan aturan baru ke daftar aturan.

   Untuk aturan yang ada, pilih aturan yang tidak sesuai dari daftar aturan dan pilih daftar dropdown Tindakan.
3. Dari daftar dropdown Tindakan, pilih Kelola remediasi. Pilih “Remediasi otomatis” dan kemudian pilih tindakan remediasi yang sesuai dari daftar.

   > **Note**
   >
   > Anda hanya dapat mengelola remediasi untuk aturan terkait AWS Config non-layanan. Untuk informasi selengkapnya, lihat Aturan Tertaut Layanan AWS.

   Bergantung pada tindakan remediasi yang dipilih, Anda melihat parameter tertentu atau tidak ada parameter.
4. Pilih Remediasi otomatis untuk memulihkan sumber daya yang tidak sesuai secara otomatis.

   Jika sumber daya masih tidak sesuai setelah perbaikan otomatis, Anda dapat mengatur aturan untuk mencoba remediasi otomatis lagi. Masukkan percobaan ulang dan detik yang diinginkan.

> **Note**
>
> Ada biaya yang terkait dengan menjalankan skrip remediasi beberapa kali. Percobaan ulang hanya terjadi jika remediasi gagal dan bekerja dalam jangka waktu yang ditentukan; misalnya, 5 percobaan ulang dalam 300 detik. Untuk informasi selengkapnya, lihat Harga Otomasi Systems Manager.

5. (Opsional): Jika Anda ingin meneruskan ID sumber daya sumber daya yang tidak sesuai ke tindakan remediasi, pilih parameter ID Sumber Daya. Jika dipilih, saat runtime parameter tersebut diganti dengan ID sumber daya yang akan diperbaiki.

   Setiap parameter memiliki nilai statis atau nilai dinamis. Jika Anda tidak memilih parameter ID sumber daya tertentu dari daftar dropdown, Anda dapat memasukkan nilai untuk setiap tombol. Jika Anda memilih parameter ID sumber daya dari daftar dropdown, Anda dapat memasukkan nilai untuk semua kunci lainnya kecuali parameter ID sumber daya yang dipilih.
6. Pilih Simpan. Halaman Aturan ditampilkan.

Untuk pemecahan masalah tindakan remediasi yang gagal

Untuk mengatasi masalah tindakan remediasi yang gagal, Anda dapat menjalankan AWS perintah Command Line Interface `describe-remediation-execution-status` untuk mendapatkan tampilan rinci Eksekusi Remediasi untuk sekumpulan sumber daya. Detailnya mencakup status, stempel waktu untuk langkah-langkah eksekusi remediasi, dan pesan kesalahan apa pun untuk langkah-langkah yang gagal.

Remediasi otomatis dapat dimulai bahkan untuk sumber daya yang sesuai

Jika Anda mengaktifkan remediasi otomatis untuk AWS Config aturan tertentu menggunakan PutRemediationConfigurationsAPI atau AWS Config konsol, aturan tersebut memulai proses remediasi untuk semua sumber daya yang tidak sesuai untuk aturan tertentu tersebut. Proses remediasi auto bergantung pada snapshot data kepatuhan yang ditangkap secara berkala. Setiap sumber daya yang tidak sesuai yang diperbarui di antara jadwal snapshot akan terus diperbaiki berdasarkan snapshot data kepatuhan terakhir yang diketahui.

Ini berarti bahwa dalam beberapa kasus remediasi otomatis dapat dimulai bahkan untuk sumber daya yang sesuai, karena prosesor bootstrap menggunakan database yang dapat memiliki hasil evaluasi basi berdasarkan snapshot data kepatuhan terakhir yang diketahui.

Setting Up Auto Remediation (API)

Gunakan operasi AWS Config API berikut untuk menyiapkan remediasi otomatis:

- PutRemediationExceptions, menambahkan pengecualian baru atau memperbarui pengecualian yang ada untuk sumber daya tertentu dengan AWS Config aturan tertentu.
- DescribeRemediationExceptions, mengembalikan rincian dari satu atau lebih pengecualian remediasi.

Menghapus Tindakan Remediasi untuk AWS Config

Anda dapat menggunakan AWS Config konsol atau AWS CLI untuk menghapus tindakan remediasi.

Deleting remediation actions (Console)

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Pilih Aturan di sebelah kiri dan kemudian pada halaman Aturan, pilih aturan dari daftar aturan dan pilih Lihat detail.
3. Pada *name of the rule* halaman, buka bagian Tindakan Remediasi. Perluas bagian untuk melihat detail tambahan.
4. Di bagian Tindakan Remediasi, pilih Hapus dan konfirmasikan tindakan penghapusan Anda.

> **Note**
>
> Jika remediasi sedang berlangsung, tindakan remediasi tidak akan dihapus. Setelah Anda memilih menghapus tindakan remediasi, Anda tidak dapat mengambil tindakan remediasi. Menghapus tindakan remediasi tidak menghapus aturan terkait.

Jika tindakan remediasi dihapus, parameter Resource ID akan kosong dan menampilkan N/A. Pada halaman Aturan, kolom tindakan remediasi menampilkan Tidak diatur untuk aturan terkait.

Deleting remediation actions (API)

Gunakan operasi AWS Config API berikut untuk menyiapkan remediasi otomatis:

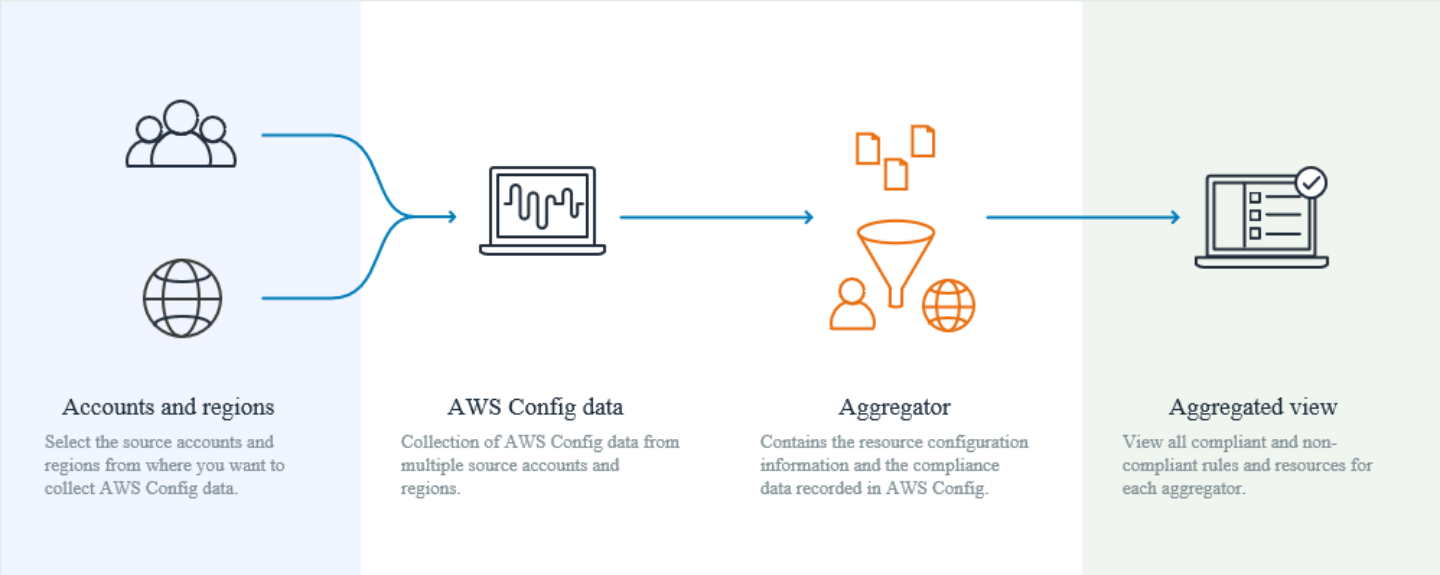
- DeleteRemediationConfiguration, menghapus konfigurasi remediasi.
- DeleteRemediationExceptions, menghapus satu atau lebih pengecualian remediasi yang disebutkan dalam kunci sumber daya.

Agregasi Data Multi-Wilayah Multi-Akun untuk AWS Config

Agregator adalah tipe AWS Config sumber daya yang mengumpulkan data AWS Config konfigurasi dan kepatuhan dari berikut ini:

- Beberapa akun dan beberapa AWS Wilayah.
- Akun tunggal dan beberapa AWS Wilayah.
- Sebuah organisasi di dalam AWS Organizations dan semua akun dalam organisasi yang telah AWS Config diaktifkan.

Gunakan agregator untuk melihat konfigurasi sumber daya dan data kepatuhan yang direkam. AWS Config Gambar berikut menampilkan bagaimana agregator mengumpulkan AWS Config data dari beberapa akun dan Wilayah.



Kasus penggunaan

- Pemantauan Kepatuhan: Anda dapat mengumpulkan data kepatuhan untuk menilai keseluruhan postur kepatuhan organisasi Anda, atau di seluruh akun dan Wilayah.
- Ubah Pelacakan: Anda dapat melacak perubahan sumber daya dari waktu ke waktu di seluruh organisasi, atau di seluruh akun dan Wilayah.
- Hubungan Sumber Daya: Anda dapat menganalisis dependensi dan hubungan sumber daya di seluruh organisasi, atau di seluruh akun dan Wilayah.

> **Note**
>
> Agregator menyediakan tampilan hanya-baca ke akun sumber dan Wilayah yang diberi wewenang untuk dilihat agregator dengan mereplikasi data dari akun sumber ke akun agregator. Agregator tidak menyediakan akses bermutasi ke akun sumber atau wilayah. Misalnya, ini berarti Anda tidak dapat menerapkan aturan melalui agregator atau mendorong file snapshot ke akun sumber atau wilayah melalui agregator.
> Menggunakan agregator tidak menimbulkan biaya tambahan.

Terminologi

Akun sumber adalah Akun AWS dari mana Anda ingin menggabungkan konfigurasi AWS Config sumber daya dan data kepatuhan. Akun sumber dapat berupa akun individu atau organisasi di AWS Organizations. Anda dapat memberikan akun sumber satu per satu atau Anda dapat mengambilnya. AWS Organizations

Wilayah sumber adalah AWS Wilayah tempat Anda ingin menggabungkan AWS Config konfigurasi dan data kepatuhan.

Akun agregator adalah akun tempat Anda membuat agregator.

Otorisasi mengacu pada izin yang Anda berikan ke akun agregator dan wilayah untuk mengumpulkan data AWS Config konfigurasi dan kepatuhan Anda. Otorisasi tidak diperlukan jika Anda menggabungkan akun sumber yang merupakan bagian dari. AWS Organizations

Agregator terkait layanan ditautkan ke yang spesifik. Layanan AWS Konfigurasi dan data kepatuhan dalam lingkup ditetapkan oleh layanan tertaut.

Support Wilayah

Saat ini, agregasi data multi-wilayah multi-akun didukung di Wilayah berikut:

Nama Wilayah	Wilayah	Titik Akhir	Protokol	
AS Timur (Ohio)	us–east-2	config.us-east-2.amazonaws.com	HTTPS	

Nama Wilayah	Wilayah	Titik Akhir	Protokol
AS Timur (Virginia Utara)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
AS Barat (Californ ia Utara)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
AS Barat (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
Afrika (Cape Town)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asia Pasifik (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asia Pasifik (Hyderaba d)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asia Pasifik (Jakarta)	ap-southe ast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asia Pasifik (Malaysia)	ap-southe ast-5	config.ap-southeast-5.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Asia Pasifik (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia Pasifik (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pasifik (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia Pasifik (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia Pasifik (Singapura)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pasifik (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pasifik (Taipei)	ap-timur-2	config.ap-east-2.amazonaws.com	HTTPS
Asia Pasifik (Thailand)	ap-tenggara 7	config.ap-southeast-7.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Kanada (Pusat)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Kanada Barat (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Eropa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Eropa (Irlandia)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Eropa (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Eropa (Milan)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Eropa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Eropa (Spanyol)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Eropa (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Eropa (Zürich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Meksiko (Tengah)	mx-pusat-1	config.mx-central-1.amazonaws.com	HTTPS
Timur Tengah (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Timur Tengah (UAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
Amerika Selatan (Sao Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (AS-Timur)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (AS-Barat)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Melihat Data Kepatuhan dan Inventaris di Dasbor Agregator untuk AWS Config

Dasbor pada halaman Agregator menampilkan data konfigurasi sumber daya gabungan AWS Anda. Ini memberikan gambaran umum tentang aturan Anda, paket kesesuaian, dan status kepatuhan mereka.

Dasbor menyediakan jumlah sumber daya total sumber AWS daya. Jenis sumber daya dan akun sumber diberi peringkat berdasarkan jumlah sumber daya tertinggi. Ini juga menyediakan hitungan aturan dan paket kesesuaian yang sesuai dan tidak patuh. Aturan yang tidak patuh diberi peringkat berdasarkan jumlah sumber daya yang tidak patuh tertinggi. Paket kesesuaian yang tidak sesuai dan akun sumber diberi peringkat berdasarkan jumlah aturan tidak patuh tertinggi.

Setelah menyiapkan AWS Config, itu mulai menggabungkan data dari akun sumber yang ditentukan menjadi agregator. Mungkin perlu beberapa menit agar status kepatuhan aturan ditampilkan.

Menggunakan Dasbor Aggregator

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Arahkan ke halaman Agregator. Anda dapat melihat:
   - Aturan Anda dan kepatuhan mereka menyatakan.
   - Paket kesesuaian Anda dan status kepatuhan mereka.
   - AWS Sumber daya Anda dan data konfigurasinya.
3. Pilih agregator dari dasbor. Filter melalui agregator Anda dengan nama agregator. Anda dapat melihat widget berikut:
   - Persediaan sumber daya

     Lihat 10 jenis sumber daya teratas dari agregator yang dipilih, dalam urutan menurun menurut jumlah sumber daya. Pilih jumlah total sumber daya untuk agregator yang dipilih, ditampilkan dalam tanda kurung setelah inventaris Sumber Daya, untuk membuka halaman Sumber Daya agregat, di mana Anda dapat melihat semua sumber daya untuk agregator. Atau, pilih jenis sumber daya di widget untuk pergi ke halaman Sumber Daya agregat, difilter menggunakan jenis sumber daya yang ditentukan.
   - Akun berdasarkan jumlah sumber daya

Lihat lima akun teratas dari aggeregator yang dipilih dalam urutan menurun menurut jumlah sumber daya. Pilih akun di widget untuk pergi ke halaman Sumber Daya, difilter menggunakan akun yang ditentukan.

- Aturan yang tidak patuh

  Lihat lima aturan teratas yang tidak sesuai dari Aggregator yang dipilih, dalam urutan menurun berdasarkan jumlah sumber daya yang tidak sesuai. Pilih aturan di widget untuk pergi ke halaman detail untuk aturan yang ditentukan. Pilih Lihat semua aturan yang tidak sesuai untuk membuka halaman Aturan agregat, tempat Anda dapat melihat semua aturan untuk agregator.

- Akun dengan aturan yang tidak patuh

  Lihat lima akun teratas dari agregator yang dipilih, dalam urutan menurun dengan jumlah aturan yang tidak sesuai. Pilih akun di widget untuk pergi ke halaman Aturan agregat, di mana Anda dapat melihat semua aturan untuk agregator yang difilter menggunakan akun yang ditentukan.

- Akun dengan paket kesesuaian yang tidak sesuai

  Lihat lima akun teratas dari agregagtor yang dipilih, dalam urutan menurun dengan jumlah paket kesesuaian yang tidak sesuai. Pilih akun di widget untuk pergi ke halaman Paket Kesesuaian agregat, di mana Anda dapat melihat semua paket kesesuaian untuk agregagtor yang difilter menggunakan akun yang ditentukan.

4. Di panel navigasi kiri, pilih salah satu opsi berikut dari menu tarik-turun:

   - Dasbor kepatuhan

     Lihat dasbor kepatuhan otomatis dengan menggunakan widget yang merangkum wawasan tentang kepatuhan sumber daya dalam agregator Anda. Anda dapat melihat data seperti 10 jenis sumber daya teratas berdasarkan sumber daya yang tidak sesuai, dan 10 paket kesesuaian tingkat akun teratas berdasarkan aturan yang tidak sesuai. Untuk informasi tentang grafik dan bagan ini, lihat Dasbor kepatuhan.

   - Paket kesesuaian

     Lihat semua paket kesesuaian yang dibuat dan ditautkan ke yang berbeda Akun AWS dalam agregator Anda. Halaman Conformance Pack menampilkan tabel yang mencantumkan nama, Wilayah, ID akun, dan status kepatuhan setiap paket kesesuaian. Dari halaman ini, Anda dapat memilih paket kesesuaian dan Lihat detail untuk informasi selengkapnya tentang aturan dan sumber daya serta status kepatuhannya.

- Aturan

  Lihat semua aturan yang dibuat dan ditautkan ke AWS akun yang berbeda dalam agregator Anda. Halaman Aturan menampilkan tabel yang mencantumkan nama, status kepatuhan, Wilayah, dan akun setiap aturan. Dari halaman ini, Anda dapat memilih aturan dan Lihat detail untuk informasi, seperti agregator, Wilayah, ID akun, dan sumber daya dalam ruang lingkup.

- Dasbor inventaris

  Lihat dasbor inventaris otomatis dengan menggunakan widget yang merangkum wawasan tentang data konfigurasi sumber daya dalam agregator Anda. Anda dapat melihat data seperti 10 jenis sumber daya teratas berdasarkan jumlah sumber daya, dan 10 akun teratas berdasarkan jumlah sumber daya. Untuk informasi tentang grafik dan bagan ini, lihat Dasbor inventaris.

- Sumber

  Lihat semua sumber daya yang direkam dan ditautkan ke AWS akun yang berbeda dalam agregator Anda. Dari halaman Sumber Daya, pilih sumber daya dan Lihat detail untuk melihat detailnya, aturan yang terkait dengannya, dan konfigurasi sumber daya saat ini. Anda juga dapat melihat informasi tentang sumber daya, seperti agregator, Wilayah, ID akun, nama sumber daya, jenis sumber daya, dan ID sumber daya.

- Otorisasi

  Lihat dan kelola semua akun yang saat ini diotorisasi atau menunggu otorisasi. Dari halaman Otorisasi, pilih Tambahkan otorisasi untuk memberikan akses ke akun lain. Pilih Hapus otorisasi untuk mencabut akses dari ID akun.

> **Note**
>
> Pemecahan Masalah
> Anda mungkin melihat pesan pengumpulan data dari semua akun sumber dan wilayah tidak lengkap ditampilkan dalam tampilan agregat karena alasan berikut:
>
> - Transfer AWS Config aturan yang tidak patuh dan data konfigurasi AWS sumber daya sedang berlangsung.
> - AWS Config tidak dapat menemukan aturan untuk mencocokkan filter yang Anda terapkan. Pilih akun atau wilayah yang sesuai, dan coba lagi.

Anda mungkin melihat pesan ini ditampilkan dalam tampilan agregat: Pengumpulan data dari organisasi Anda tidak lengkap. Anda dapat melihat data di bawah ini hanya selama 24 jam. Ini ditampilkan karena alasan berikut:

- AWS Config tidak dapat mengakses detail organisasi Anda karena peran IAM yang tidak valid. Jika peran IAM tetap tidak valid selama lebih dari 24 jam, AWS Config menghapus data untuk seluruh organisasi.
- AWS Config akses layanan dinonaktifkan di organisasi Anda.

Dasbor Kepatuhan

Lihat dasbor kepatuhan otomatis dengan menggunakan widget yang merangkum wawasan tentang kepatuhan sumber daya dalam agregator Anda Dasbor ini hanya menampilkan aturan dengan hasil kepatuhan.

> **Note**
>
> Batasan
>
> Wawasan di dasbor kepatuhan disediakan oleh fitur Kueri Lanjutan AWS Config, dan fitur ini tidak mendukung struktur bersarang atau membongkar array bersarang. Ini berarti bahwa dasbor kepatuhan menampilkan kepatuhan keseluruhan sumber daya dan bukan status kepatuhan untuk setiap aturan tertentu yang melaporkan sumber daya.
>
> Misalnya, jika Anda memeriksa item konfigurasi (CI) untuk jenis sumber daya`AWS::Config::ResourceCompliance`, dasbor akan menampilkan hasil kepatuhan untuk semua aturan yang melaporkan sumber daya tersebut. Jika ada 10 aturan yang melaporkan sumber daya, 9 di antaranya adalah COMPLIANT, dan hanya 1 yang NON_COMPLIANT, kepatuhan keseluruhan sumber daya tersebut adalah NON_COMPLIANT.

Ringkasan Kepatuhan Berdasarkan Sumber Daya

Menampilkan diagram lingkaran yang membandingkan jumlah sumber daya yang sesuai dengan sumber daya yang tidak sesuai dari agregator yang dipilih. Arahkan kursor ke grafik untuk melihat jumlah dan persentase yang tepat dari sumber daya yang sesuai dan tidak sesuai.

Data yang ditampilkan tergantung pada pengaturan perekam konfigurasi untuk setiap akun di agregator yang dipilih, dan Wilayah tempat agregator yang dipilih dikonfigurasi untuk mengumpulkan data.

10 jenis sumber daya teratas berdasarkan sumber daya yang tidak sesuai

Menampilkan grafik batang horizontal yang membandingkan hingga 10 jenis sumber daya dari agregator yang dipilih dalam urutan menurun dengan jumlah sumber daya yang tidak sesuai. Arahkan kursor ke grafik untuk melihat jumlah pasti sumber daya yang tidak sesuai untuk setiap jenis sumber daya.

Data yang ditampilkan tergantung pada pengaturan perekam konfigurasi untuk setiap akun di agregator yang dipilih dan Wilayah tempat agregator yang dipilih dikonfigurasi untuk mengumpulkan data.

10 akun teratas berdasarkan sumber daya yang tidak sesuai

10 akun teratas berdasarkan sumber daya yang tidak sesuai menampilkan grafik batang horizontal yang membandingkan hingga 10 akun dari agregator yang dipilih dalam urutan menurun dengan jumlah sumber daya yang tidak sesuai. Arahkan kursor ke grafik untuk melihat jumlah pasti sumber daya yang tidak sesuai untuk setiap akun.

Data yang ditampilkan tergantung pada pengaturan perekam konfigurasi untuk setiap akun di agregator yang dipilih, dan Wilayah tempat agregator yang dipilih dikonfigurasi untuk mengumpulkan data.

10 wilayah teratas berdasarkan sumber daya yang tidak sesuai

Menampilkan grafik batang horizontal yang membandingkan hingga 10 Wilayah tempat agregator yang dipilih mengumpulkan data dalam urutan menurun dengan jumlah sumber daya yang tidak sesuai. Arahkan kursor ke grafik untuk melihat jumlah pasti sumber daya yang tidak sesuai untuk setiap Wilayah.

Data yang ditampilkan tergantung pada pengaturan perekam konfigurasi untuk setiap akun di agregator yang dipilih.

10 paket kesesuaian tingkat akun teratas berdasarkan aturan yang tidak sesuai

Menampilkan grafik batang horizontal yang membandingkan hingga 10 paket kesesuaian tingkat akun dari agregator yang dipilih dalam urutan menurun dengan jumlah aturan yang tidak sesuai. Arahkan kursor ke grafik untuk melihat persentase aturan yang sesuai dan tidak patuh untuk setiap paket kesesuaian tingkat akun.

Data yang ditampilkan tergantung pada pengaturan perekam konfigurasi untuk setiap akun di agregator yang dipilih, dan Wilayah tempat agregator yang dipilih dikonfigurasi untuk mengumpulkan data.

10 paket kesesuaian tingkat organisasi teratas menurut aturan yang tidak patuh

Menampilkan grafik batang horizontal yang membandingkan hingga 10 paket kesesuaian tingkat organisasi dari agregator yang dipilih dalam urutan menurun dengan jumlah aturan yang tidak sesuai. Arahkan kursor ke grafik untuk melihat persentase aturan yang sesuai dan tidak patuh di setiap paket kesesuaian tingkat organisasi.

Data yang ditampilkan tergantung pada pengaturan perekam konfigurasi untuk setiap akun di agregator yang dipilih dan Wilayah tempat agregator yang dipilih dikonfigurasi untuk mengumpulkan data.

10 akun teratas berdasarkan aturan yang tidak patuh di seluruh paket kesesuaian

10 akun teratas berdasarkan aturan yang tidak sesuai di seluruh paket kesesuaian menampilkan grafik batang horizontal yang membandingkan hingga 10 akun dari agregator yang dipilih dalam urutan menurun dengan jumlah aturan yang tidak sesuai di semua paket kesesuaian Anda. Arahkan kursor ke grafik untuk melihat jumlah pasti aturan yang tidak sesuai di setiap akun.

Data yang ditampilkan tergantung pada pengaturan perekam konfigurasi untuk setiap akun di agregator yang dipilih dan Wilayah tempat agregator yang dipilih dikonfigurasi untuk mengumpulkan data.

Dasbor Inventaris

Lihat dasbor inventaris otomatis dengan menggunakan widget yang merangkum wawasan tentang data konfigurasi sumber daya dalam agregator Anda.

10 jenis sumber daya teratas berdasarkan jumlah sumber daya

Menampilkan grafik batang horizontal yang membandingkan hingga 10 jenis sumber daya dari agregator yang dipilih dalam urutan menurun berdasarkan jumlah sumber daya. Arahkan kursor ke grafik untuk melihat jumlah sumber daya yang tepat untuk setiap jenis sumber daya.

Data yang ditampilkan tergantung pada pengaturan perekam konfigurasi untuk setiap akun di agregator yang dipilih, dan Wilayah tempat agregator yang dipilih dikonfigurasi untuk mengumpulkan data.

Jumlah sumber daya berdasarkan wilayah

Menampilkan grafik batang horizontal yang membandingkan hingga 10 Wilayah tempat agregator yang dipilih mengumpulkan data dalam urutan menurun berdasarkan jumlah sumber daya. Arahkan kursor ke grafik untuk melihat jumlah sumber daya yang tepat untuk setiap Wilayah.

Data yang ditampilkan tergantung pada pengaturan perekam konfigurasi untuk setiap akun di agregator yang dipilih.

10 akun teratas berdasarkan jumlah sumber daya

Menampilkan grafik batang horizontal yang membandingkan hingga 10 akun dari agregator yang dipilih dalam urutan menurun berdasarkan jumlah sumber daya. Arahkan kursor ke grafik untuk melihat sumber daya angka yang tepat untuk setiap jenis sumber daya.

Data yang ditampilkan tergantung pada pengaturan perekam konfigurasi untuk setiap akun di agregator yang dipilih dan Wilayah tempat agregator yang dipilih dikonfigurasi untuk mengumpulkan data.

Jumlah sumber daya menurut jenis sumber daya EC2 layanan Amazon

Menampilkan grafik batang horizontal yang membandingkan jenis EC2 sumber daya Amazon dari agregator yang dipilih dalam urutan menurun menurut jumlah sumber daya. Arahkan kursor ke grafik untuk melihat jumlah sumber daya yang tepat untuk setiap jenis EC2 sumber daya Amazon.

Data yang ditampilkan tergantung pada pengaturan perekam konfigurasi untuk setiap akun di agregator yang dipilih, dan Wilayah tempat agregator yang dipilih dikonfigurasi untuk mengumpulkan data. Untuk menggunakan bagan ini, Anda harus mengonfigurasi perekam untuk merekam jenis EC2 sumber daya Amazon. Untuk informasi selengkapnya, lihat Memilih AWS Config Rekaman Sumber Daya yang mana.

10 jenis EC2 instans teratas yang digunakan

Menampilkan grafik batang horizontal yang membandingkan hingga 10 jenis EC2 instans Amazon dari agregator yang dipilih dalam urutan menurun berdasarkan penggunaan. Arahkan kursor ke grafik untuk melihat penggunaan untuk setiap jenis EC2 instance.

Data yang ditampilkan tergantung pada pengaturan perekam konfigurasi untuk setiap akun di agregator yang dipilih dan Wilayah tempat agregator yang dipilih dikonfigurasi untuk mengumpulkan data. Untuk menggunakan bagan ini, Anda harus mengonfigurasi perekam untuk merekam jenis sumber daya EC2 instance. Untuk informasi selengkapnya, lihat Pengodean ulang AWS Sumber Daya.

EBS Volume dihitung berdasarkan jenis dan ukuran volume

Menampilkan grafik batang vertikal yang membandingkan volume EBS dari agregator yang dipilih berdasarkan jumlah sumber daya. Arahkan kursor ke grafik untuk melihat hitungan dan rincian ukuran untuk setiap jenis volume EBS.

Data yang ditampilkan tergantung pada pengaturan perekam konfigurasi untuk setiap akun di agregator yang dipilih dan Wilayah tempat agregator yang dipilih dikonfigurasi untuk mengumpulkan data. Untuk menggunakan bagan ini, Anda harus mengonfigurasi perekam untuk merekam jenis sumber daya EC2 volume. Untuk informasi selengkapnya, lihat Memilih AWS Config Rekaman Sumber Daya yang mana.

Jumlah EC2 instance yang berjalan vs. dihentikan menurut jenis

Menampilkan grafik batang horizontal yang membandingkan jenis EC2 instance dari agregator yang dipilih yang berjalan ke EC2 instance yang dihentikan berdasarkan jenis instance. Arahkan kursor ke grafik untuk melihat jumlah persis EC2 instance berhenti dan berjalan untuk setiap jenis.

Data yang ditampilkan tergantung pada pengaturan perekam konfigurasi untuk setiap akun di agregator yang dipilih dan Wilayah tempat agregator yang dipilih dikonfigurasi untuk mengumpulkan data. Untuk menggunakan bagan ini, Anda harus mengonfigurasi perekam untuk merekam jenis sumber daya EC2 instance. Untuk informasi selengkapnya, lihat Pengodean ulang AWS Sumber Daya.

Membuat Agregator untuk AWS Config

Anda dapat menggunakan AWS Config konsol atau AWS CLI untuk membuat agregator Anda. Dari AWS Config Anda dapat memilih Tambahkan akun individual IDs atau Tambahkan organisasi saya dari tempat Anda ingin menggabungkan data. Untuk AWS CLI ada dua prosedur yang berbeda.

Creating Aggregators (Console)

Pada halaman Aggregator, Anda dapat membuat agregator dengan menentukan akun sumber IDs atau organisasi dan wilayah tempat Anda ingin mengumpulkan data.

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Arahkan ke halaman Agregator dan pilih Buat agregator.
3. Izinkan replikasi data, memberikan izin AWS Config untuk mereplikasi data dari akun sumber ke akun agregator.

Pilih Izinkan AWS Config untuk mereplikasi data dari akun sumber ke akun agregator. Anda harus memilih kotak centang ini untuk terus menambahkan agregator.

4. Untuk nama Aggregator, ketikkan nama untuk agregator Anda.

   Nama agregator harus berupa nama unik dengan maksimal 64 karakter alfanumerik. Nama itu dapat berisi tanda hubung dan garis bawah.

5. Untuk Pilih akun sumber, pilih Tambahkan akun individual IDs atau Tambahkan organisasi saya dari tempat Anda ingin mengumpulkan data.

   > **Note**
   >
   > Otorisasi diperlukan saat menggunakan Tambahkan akun individual IDs untuk memilih akun sumber.

   - Jika Anda memilih Tambahkan akun individual IDs, Anda dapat menambahkan akun individual IDs untuk akun agregator.
     1. Pilih Tambahkan akun sumber untuk menambahkan akun IDs.
     2. Pilih Tambahkan Akun AWS IDs untuk menambahkan dipisahkan koma Akun AWS IDs secara manual. Jika Anda ingin mengumpulkan data dari akun saat ini, ketikkan ID akun akun tersebut.

        ATAU

        Pilih Unggah file untuk mengunggah file (.txt atau .csv) yang dipisahkan koma. Akun AWS IDs
     3. Pilih Tambahkan akun sumber untuk mengonfirmasi pilihan Anda.
   - Jika Anda memilih Tambahkan organisasi saya, Anda dapat menambahkan semua akun di organisasi Anda ke akun agregator.

     > **Note**
     >
     > Anda harus masuk ke akun manajemen atau administrator yang didelegasikan terdaftar dan semua fitur harus diaktifkan di organisasi Anda. Jika pemanggil adalah akun manajemen, AWS Config panggil `EnableAwsServiceAccess` API untuk mengaktifkan integrasi antara AWS Config dan AWS Organizations.

Jika pemanggil adalah administrator terdelegasi terdaftar, AWS Config panggil `ListDelegatedAdministrators` API untuk memverifikasi apakah pemanggil adalah administrator delegasi yang valid.
Pastikan akun manajemen mendaftarkan administrator yang didelegasikan untuk nama utama AWS Config layanan (config.amazonaws.com) sebelum administrator yang didelegasikan membuat agregator. Untuk mendaftarkan administrator yang didelegasikan, lihatMendaftarkan Administrator Delegasi untuk AWS Config.

Anda harus menetapkan peran IAM untuk memungkinkan panggilan read-only AWS Config APIs untuk organisasi Anda.

1. Pilih Pilih peran dari akun Anda untuk memilih peran IAM yang ada.

> **Note**
>
> Di konsol IAM, lampirkan kebijakan `AWSConfigRoleForOrganizations` terkelola ke peran IAM Anda. Melampirkan kebijakan ini memungkinkan AWS Config untuk menelepon AWS Organizations `DescribeOrganization`,`ListAWSServiceAccessForOrganization`, dan `ListAccounts` APIs. Secara default `config.amazonaws.com` secara otomatis ditentukan sebagai entitas tepercaya.

2. Atau, pilih Buat peran dan ketik nama untuk nama peran IAM Anda untuk membuat peran IAM.

6. Untuk Wilayah, pilih wilayah yang ingin Anda agregat datanya.
   - Pilih satu wilayah atau beberapa wilayah atau semua Wilayah AWS.
   - Pilih Sertakan data future Wilayah AWS to aggregate from all future Wilayah AWS di mana agregasi data multi-wilayah multi-akun diaktifkan.
7. Pilih Simpan. AWS Config menampilkan agregator.

Creating Aggregators using Individual Accounts (AWS CLI)

1. Buka jendela command prompt atau terminal.
2. Masukkan perintah berikut untuk membuat agregator bernama**`MyAggregator`**.

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
 MyAggregator --account-aggregation-sources "[{\"AccountIds\": [\"AccountID1\",
\"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"
```

Untuk`account-aggregation-sources`, masukkan salah satu dari berikut ini.

- Daftar dipisahkan koma yang ingin Anda agregat datanya. Akun AWS IDs Bungkus akun IDs dalam tanda kurung siku, dan pastikan untuk menghindari tanda kutip (misalnya,`"[{\"AccountIds\": [\"AccountID1\",\"AccountID2\", \"AccountID3\"],\"AllAwsRegions\": true}]"`).
- Anda juga dapat mengunggah file JSON yang dipisahkan koma Akun AWS IDs. Unggah file menggunakan sintaks berikut: `--account-aggregation-sources MyFilePath/MyFile.json`

  File JSON harus dalam format berikut:

```
[
    {
        "AccountIds": [
            "AccountID1",
            "AccountID2",
            "AccountID3"
        ],
        "AllAwsRegions": true
    }
]
```

3. Tekan Enter untuk menjalankan perintah.

   Anda akan melihat output yang serupa dengan yang berikut:

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "AccountAggregationSources": [
            {
```

```
                "AllAwsRegions": true,
                "AccountIds": [
                    "AccountID1",
                    "AccountID2",
                    "AccountID3"
                ]
            }
        ],
        "LastUpdatedTime": 1517942461.442
    }
}
```

Creating Aggregators using AWS Organizations (AWS CLI)

Sebelum memulai prosedur ini, Anda harus masuk ke akun manajemen atau administrator yang didelegasikan terdaftar dan semua fitur harus diaktifkan di organisasi Anda.

> **Note**
>
> Pastikan akun manajemen mendaftarkan administrator yang didelegasikan dengan kedua nama utama AWS Config layanan berikut (`config.amazonaws.com`dan`config-multiaccountsetup.amazonaws.com`) sebelum administrator yang didelegasikan membuat agregator. Untuk mendaftarkan administrator yang didelegasikan, lihat[Mendaftarkan Administrator Delegasi untuk AWS Config](#).

1. Buka jendela command prompt atau terminal.
2. Jika belum membuat peran IAM untuk AWS Config agregator Anda, masukkan perintah berikut:

```
aws iam create-role --role-name OrgConfigRole --assume-role-policy-document
 "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":\"\",\"Effect\":\"Allow\",
\"Principal\":{\"Service\":\"config.amazonaws.com\"},\"Action\":\"sts:AssumeRole
\"}]}" --description "Role for organizational AWS Config aggregator"
```

> **Note**
>
> Salin Nama Sumber Daya Amazon (ARN) dari peran IAM ini untuk digunakan saat Anda membuat agregator. AWS Config Anda dapat menemukan ARN pada objek respons.

3. Jika belum melampirkan kebijakan ke peran IAM Anda, lampirkan kebijakan AWSConfigRoleForOrganizationsterkelola atau masukkan perintah berikut:

```
aws iam create-policy --policy-name OrgConfigPolicy --policy-document
 '{"Version":"2012-10-17","Statement":[{"Effect":"Allow","Action":
["organizations:ListAccounts","organizations:DescribeOrganization","organizations:ListAW
```

4. Masukkan perintah berikut untuk membuat agregator bernama**MyAggregator**.

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
 MyAggregator --organization-aggregation-source "{\"RoleArn\": \"Complete-Arn\",
\"AllAwsRegions\": true}"
```

5. Tekan Enter untuk menjalankan perintah.

   Anda akan melihat output yang serupa dengan yang berikut:

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

Mendaftarkan Administrator Delegasi untuk AWS Config

Administrator yang didelegasikan adalah akun dalam AWS Organisasi tertentu yang diberikan hak administratif tambahan untuk layanan tertentu. AWS Untuk informasi selengkapnya, lihat Administrator yang didelegasikan di Panduan AWS Organizations Pengguna. Anda harus menggunakan AWS CLI untuk mendaftarkan administrator yang didelegasikan.

Mendaftarkan Administrator yang Delegasi

1. Masuk dengan kredensi akun manajemen.
2. Buka jendela command prompt atau terminal.
3. Masukkan perintah berikut untuk mengaktifkan akses layanan sebagai administrator yang didelegasikan agar organisasi Anda dapat menerapkan dan mengelola AWS Config aturan serta paket kesesuaian di seluruh organisasi Anda:

```
aws organizations enable-aws-service-access --service-principal=config-
multiaccountsetup.amazonaws.com
```

4. Masukkan perintah berikut untuk mengaktifkan akses layanan sebagai administrator yang didelegasikan bagi organisasi Anda untuk mengumpulkan AWS Config data di seluruh organisasi Anda:

```
aws organizations enable-aws-service-access --service-
principal=config.amazonaws.com
```

5. Untuk memeriksa apakah akses layanan aktifkan selesai, masukkan perintah berikut dan tekan Enter untuk menjalankan perintah.

```
aws organizations list-aws-service-access-for-organization
```

Anda akan melihat output yang serupa dengan yang berikut:

```
{
    "EnabledServicePrincipals": [
        {
            "ServicePrincipal": [
                "config.amazonaws.com",
                "config-multiaccountsetup.amazonaws.com"
        ],
```

```
            "DateEnabled": 1607020860.881
        }
    ]
}
```

6. Selanjutnya, masukkan perintah berikut untuk mendaftarkan akun anggota sebagai administrator yang didelegasikan untuk AWS Config.

```
aws organizations register-delegated-administrator --service-principal=config-
multiaccountsetup.amazonaws.com --account-id MemberAccountID
```

and

```
aws organizations register-delegated-administrator --service-
principal=config.amazonaws.com --account-id MemberAccountID
```

7. Untuk memeriksa apakah pendaftaran administrator yang didelegasikan selesai, masukkan perintah berikut dari akun manajemen dan tekan Enter untuk menjalankan perintah.

```
aws organizations list-delegated-administrators --service-principal=config-
multiaccountsetup.amazonaws.com
```

and

```
aws organizations list-delegated-administrators --service-
principal=config.amazonaws.com
```

Anda akan melihat output yang serupa dengan yang berikut:

```
{
    "DelegatedAdministrators": [
        {
            "Id": "MemberAccountID",
            "Arn": "arn:aws:organizations::ManagementAccountID:account/o-
c7esubdi38/MemberAccountID",
            "Email": "name@amazon.com",
            "Name": "name",
            "Status": "ACTIVE",
            "JoinedMethod": "INVITED",
            "JoinedTimestamp": 1604867734.48,
            "DelegationEnabledDate": 1607020986.801
```

```
        }
    ]
}
```

Mengedit Agregator untuk AWS Config

Anda dapat menggunakan AWS Config konsol atau AWS CLI untuk mengedit agregator Anda.

Editing Aggregators (Console)

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Arahkan ke halaman Aggregator, dan pilih nama agregator.
3. Pilih Tindakan dan kemudian pilih Edit.
4. Gunakan bagian pada halaman Edit agregator untuk mengubah akun sumber, peran IAM, atau wilayah untuk agregator.

   > **Note**
   >
   > Anda tidak dapat mengubah jenis sumber dari akun individual ke organisasi dan sebaliknya.

5. Pilih Simpan.

Editing Aggregators (AWS CLI)

1. Anda dapat menggunakan `put-configuration-aggregator` perintah untuk memperbarui atau mengedit agregator konfigurasi.

   Masukkan perintah berikut untuk menambahkan ID akun baru ke**`MyAggregator`**:

   ```
   aws configservice put-configuration-aggregator --configuration-aggregator-name
    MyAggregator --account-aggregation-sources "[{\"AccountIds\": [\"AccountID1\",
   \"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"
   ```

2. Bergantung pada akun sumber Anda, Anda akan melihat output yang mirip dengan berikut ini:

Untuk akun individu

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-xz2upuu6",
        "CreationTime": 1517952090.769,
        "ConfigurationAggregatorName": "MyAggregator",
        "AccountAggregationSources": [
            {
                "AllAwsRegions": true,
                "AccountIds": [
                    "AccountID1",
                    "AccountID2",
                    "AccountID3",
                    "AccountID4"
                ]
            }
        ],
        "LastUpdatedTime": 1517952566.445
    }
}
```

ATAU

Untuk sebuah organisasi

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

Menghapus Agregator untuk AWS Config

Anda dapat menggunakan AWS Config konsol atau AWS CLI untuk menghapus agregator Anda.

Deleting Aggregators (Console)

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Arahkan ke halaman Aggregator, dan pilih nama agregator.
3. Pilih Tindakan dan kemudian pilih Hapus.

   Pesan peringatan ditampilkan. Menghapus agregator mengakibatkan hilangnya semua data agregat. Anda tidak dapat memulihkan data ini tetapi data di akun sumber tidak terpengaruh.
4. Pilih Hapus untuk mengonfirmasi pilihan Anda.

Deleting Aggregators (AWS CLI)

Masukkan perintah berikut:

```
aws configservice delete-configuration-aggregator --configuration-aggregator-name
 MyAggregator
```

Jika berhasil, perintah dijalankan tanpa output tambahan.

Mengotorisasi Akun Agregator untuk Mengumpulkan Data AWS Config Konfigurasi dan Kepatuhan

Otorisasi mengacu pada izin yang Anda berikan ke akun agregator dan wilayah untuk mengumpulkan data AWS Config konfigurasi dan kepatuhan Anda. Otorisasi tidak diperlukan jika Anda menggabungkan akun sumber yang merupakan bagian dari. AWS Organizations Anda dapat menggunakan AWS Config konsol atau AWS CLI untuk mengotorisasi akun agregator.

Topik

- Pertimbangan
- Menambahkan Otorisasi

Pertimbangan

Ada dua jenis agregator: agregator akun individu dan agregator organisasi

Untuk agregator akun individual, otorisasi diperlukan untuk semua akun sumber dan Wilayah yang ingin Anda sertakan, termasuk akun eksternal dan akun anggota Wilayah dan Organisasi serta Wilayah.

Untuk agregator organisasi, otorisasi tidak diperlukan untuk wilayah akun anggota Organisasi karena otorisasi terintegrasi dengan layanan. AWS Organizations

Agregator tidak secara otomatis mengaktifkan AWS Config atas nama Anda

AWS Config perlu diaktifkan di akun sumber dan Wilayah untuk kedua jenis agregator, agar AWS Config data dihasilkan di akun sumber dan Wilayah.

Menambahkan Otorisasi

Adding Authorization (Console)

Anda dapat menambahkan otorisasi untuk memberikan izin ke akun agregator dan Wilayah untuk mengumpulkan data AWS Config konfigurasi dan kepatuhan.

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Arahkan ke halaman Otorisasi dan pilih Tambahkan otorisasi.
3. Untuk akun Aggregator, ketikkan 12 digit ID akun agregator.
4. Untuk wilayah Aggregator, pilih Wilayah AWS tempat akun agregator diizinkan untuk mengumpulkan konfigurasi AWS Config dan data kepatuhan.
5. Pilih Tambahkan otorisasi untuk mengonfirmasi pilihan Anda.

   AWS Config menampilkan akun agregator, Wilayah, dan status otorisasi.

   > **Note**
   >
   > Anda juga dapat menambahkan otorisasi ke akun agregator dan Wilayah secara terprogram menggunakan AWS CloudFormation templat sampel. Untuk informasi selengkapnya, lihat AWS::Config::AggregationAuthorization di AWS CloudFormation Panduan Pengguna.

Authorizing a Pending Request (Console)

Jika Anda memiliki permintaan otorisasi yang tertunda dari akun agregator yang ada, Anda akan melihat status permintaan di halaman Otorisasi. Anda dapat mengotorisasi permintaan yang tertunda dari halaman ini.

1. Pilih akun agregator yang ingin Anda otorisasi, lalu pilih Otorisasi.

   Pesan konfirmasi ditampilkan untuk mengonfirmasi bahwa Anda ingin memberikan izin akun agregator untuk mengumpulkan AWS Config data dari akun ini.
2. Pilih Otorisasi lagi untuk mengonfirmasi bahwa Anda ingin memberikan izin ke akun agregator.

   Status otorisasi berubah dari Meminta otorisasi ke Otorisasi.

Periode persetujuan otorisasi

Persetujuan otorisasi diperlukan untuk menambahkan akun sumber ke agregator akun individu. Permintaan persetujuan otorisasi yang tertunda akan tersedia selama 7 hari setelah agregator akun individu menambahkan akun sumber.

Adding Authorization (AWS CLI)

1. Buka jendela command prompt atau terminal.
2. Masukkan perintah berikut:

```
aws configservice put-aggregation-authorization --authorized-account-id
  AccountID --authorized-aws-region Region
```

3. Anda akan melihat output yang serupa dengan yang berikut:

```
{
    "AggregationAuthorization": {
        "AuthorizedAccountId": "AccountID",
        "AggregationAuthorizationArn":
 "arn:aws:config:Region:AccountID:aggregation-authorization/AccountID/Region",
        "CreationTime": 1518116709.993,
        "AuthorizedAwsRegion": "Region"
    }
}
```

Menghapus Otorisasi Akun Agregator untuk Mengumpulkan Data AWS Config Konfigurasi dan Kepatuhan

Otorisasi mengacu pada izin yang Anda berikan ke akun agregator dan wilayah untuk mengumpulkan data AWS Config konfigurasi dan kepatuhan Anda. Otorisasi tidak diperlukan jika Anda menggabungkan akun sumber yang merupakan bagian dari. AWS Organizations Anda dapat menggunakan AWS Config konsol atau AWS CLI untuk menghapus otorisasi.

Topik

- Pertimbangan
- Menghapus Otorisasi

Pertimbangan

Ada dua jenis agregator: agregator akun individu dan agregator organisasi

Untuk agregator akun individual, otorisasi diperlukan untuk semua akun sumber dan Wilayah yang ingin Anda sertakan, termasuk akun eksternal dan akun anggota Wilayah dan Organisasi serta Wilayah.

Untuk agregator organisasi, otorisasi tidak diperlukan untuk wilayah akun anggota Organisasi karena otorisasi terintegrasi dengan layanan. AWS Organizations

Agregator tidak secara otomatis mengaktifkan AWS Config atas nama Anda

AWS Config perlu diaktifkan di akun sumber dan Wilayah untuk kedua jenis agregator, agar AWS Config data dihasilkan di akun sumber dan Wilayah.

Menghapus Otorisasi

Deleting Authorization (Console)

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Pilih akun agregator yang ingin Anda hapus otorisasi, lalu pilih Hapus.

   Pesan peringatan ditampilkan. Saat Anda menghapus otorisasi ini, AWS Config data tidak akan lagi dibagikan dengan akun agregator.

3. Pilih Hapus lagi untuk mengonfirmasi pilihan Anda.

   Akun agregator sekarang dihapus.

Deleting Authorization (AWS CLI)

Masukkan perintah berikut:

```
aws configservice delete-aggregation-authorization --authorized-account-id
  AccountID --authorized-aws-region Region
```

Jika berhasil, perintah dijalankan tanpa output tambahan.

Melihat Agregator untuk AWS Config

Anda dapat menggunakan AWS Config konsol atau AWS CLI untuk melihat agregator Anda.

Viewing Aggregators (Console)

Untuk melihat paket kesesuaian Anda di, lihat Dasbor AWS Management Console Agregator.

Viewing Aggregators (AWS CLI)

1. Masukkan perintah berikut:

   ```
   aws configservice describe-configuration-aggregators
   ```

2. Bergantung pada akun sumber Anda, Anda akan melihat output yang mirip dengan berikut ini:

   Untuk akun individu

   ```
   {
       "ConfigurationAggregators": [
           {
               "ConfigurationAggregatorArn":
    "arn:aws:config:Region:AccountID:config-aggregator/config-aggregator-floqpus3",
               "CreationTime": 1517942461.442,
               "ConfigurationAggregatorName": "MyAggregator",
               "AccountAggregationSources": [
                   {
   ```

```
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        }
    ]
}
```

ATAU

Untuk sebuah organisasi

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

Pemecahan Masalah untuk Agregasi Data Multi-Wilayah Multi-Akun untuk AWS Config

AWS Config mungkin tidak mengumpulkan data dari akun sumber karena salah satu alasan berikut:

Jika ini terjadi	Lakukan hal berikut
AWS Config tidak diaktifkan di akun sumber untuk akun dalam Organisasi.	Aktifkan AWS Config di akun sumber dan otorisasi akun agregator untuk mengumpulkan data.
Otorisasi tidak diberikan ke akun agregator.	Masuk ke akun sumber dan berikan otorisasi ke akun agregator untuk mengumpulkan AWS Config data.
Mungkin ada masalah sementara yang mencegah agregasi data.	Agregasi data dapat mengalami penundaan. Tunggu beberapa menit.

AWS Config mungkin tidak mengumpulkan data dari organisasi karena salah satu alasan berikut:

Jika ini terjadi	Lakukan hal berikut
AWS Config tidak dapat mengakses detail organisasi Anda karena peran IAM tidak valid.	Buat peran IAM atau pilih peran IAM yang valid dari daftar peran IAM. **Note** Jika peran IAM tidak valid selama lebih dari 7 hari, AWS Config menghapus data untuk seluruh organisasi.
AWS Config akses layanan dinonaktifkan di organisasi Anda.	Anda dapat mengaktifkan integrasi antara AWS Config dan AWS Organizations melalui `EnableAWSServiceAccess` API. Jika Anda memilih Tambahkan organisasi saya di konsol, AWS Config secara otomatis mengaktifkan integrasi antara AWS Config dan AWS Organizations.
AWS Config tidak dapat mengakses detail organisasi Anda karena semua fitur tidak diaktifkan di organisasi Anda.	Aktifkan semua fitur di AWS Organizations konsol.

Jika ini terjadi	Lakukan hal berikut
Perubahan organisasi seperti menambahkan akun, menghapus akun, mengaktifkan akses layanan, dan menonaktifkan akses layanan tidak segera diperbarui di wilayah Timur Tengah (Bahrain) dan Asia Pasifik (Hong Kong).	Perubahan organisasi tunduk pada penundaan 2 jam. Tunggu selama 2 jam untuk melihat semua perubahan organisasi.

Menanyakan Status Konfigurasi AWS Sumber Daya Saat Ini dengan AWS Config

Memperkenalkan fitur pratinjau untuk kueri lanjutan yang memungkinkan Anda menggunakan kemampuan kecerdasan buatan generatif (AI generatif) untuk memasukkan petunjuk dalam bahasa Inggris biasa dan mengubahnya menjadi format kueri. ready-to-use Untuk informasi selengkapnya, lihat Pemroses kueri bahasa alami untuk kueri lanjutan.

Anda dapat menggunakan AWS Config untuk menanyakan status konfigurasi sumber AWS daya saat ini berdasarkan properti konfigurasi untuk satu akun dan Wilayah atau di beberapa akun dan Wilayah. Anda dapat melakukan kueri berbasis properti terhadap metadata status AWS sumber daya saat ini di seluruh daftar sumber daya yang mendukung. AWS Config Untuk informasi selengkapnya tentang daftar jenis sumber daya yang didukung, lihat Jenis Sumber Daya yang Didukung untuk Kueri Lanjutan.

Kueri lanjutan menyediakan satu titik akhir kueri dan bahasa kueri untuk mendapatkan metadata status sumber daya saat ini tanpa melakukan panggilan API deskripsi khusus layanan. Anda dapat menggunakan agregator konfigurasi untuk menjalankan kueri yang sama dari akun pusat di beberapa akun dan Wilayah. AWS

Topik

- Fitur
- Komponen Kueri untuk AWS Config
- Kueri Menggunakan Editor Kueri SQL untuk AWS Config (Konsol)
- Query Menggunakan SQL Query Editor untuk AWS Config ()AWS CLI
- Prosesor kueri bahasa alami untuk kueri AWS Config tingkat lanjut
- Contoh Query untuk AWS Config
- Contoh Pertanyaan Hubungan untuk AWS Config
- Batasan
- Perilaku notation/IP rentang CIDR untuk kueri lanjutan
- Beberapa properti dalam perilaku array untuk kueri lanjutan

- Support Wilayah

Fitur

AWS Config menggunakan subset `SELECT` sintaks bahasa kueri terstruktur (SQL) untuk melakukan kueri dan agregasi berbasis properti pada data item konfigurasi (CI) saat ini. Kueri berkisar dalam kompleksitas dari kecocokan terhadap pengidentifikasi and/or sumber daya tag, hingga kueri yang lebih kompleks, seperti melihat semua bucket Amazon S3 yang menonaktifkan versi. Ini memungkinkan Anda untuk menanyakan dengan tepat status sumber daya saat ini yang Anda butuhkan tanpa melakukan AWS panggilan API khusus layanan.

Ini mendukung fungsi agregasi seperti`AVG`,,`COUNT`, `MAXMIN`, dan`SUM`.

Anda dapat menggunakan kueri lanjutan untuk:

- Manajemen inventaris; misalnya, untuk mengambil daftar EC2 instans Amazon dengan ukuran tertentu.
- Keamanan dan intelijen operasional; misalnya, untuk mengambil daftar sumber daya yang memiliki properti konfigurasi tertentu diaktifkan atau dinonaktifkan.
- Optimalisasi biaya; misalnya, untuk mengidentifikasi daftar volume Amazon EBS yang tidak dilampirkan ke EC2 instance apa pun.
- Data kepatuhan; misalnya, untuk mengambil daftar semua paket kesesuaian Anda dan status kepatuhannya.

Untuk informasi tentang cara menggunakan AWS SQL Query Language, lihat Apa itu SQL (Structured Query Language)? .

Komponen Kueri untuk AWS Config

Komponen `SELECT` query SQL untuk query AWS Config lanjutan adalah sebagai berikut.

Sinopsis

```
SELECT property [, ...]
[ WHERE condition ]
[ GROUP BY property ]
```

```
[ ORDER BY property [ ASC | DESC ] [, property [ ASC | DESC ] ...] ]
```

Parameter

[syarat WHERE]

Filter hasil sesuai dengan yang `condition` Anda tentukan.

Operator perbandingan

- =(sama)
- `IN`(daftar keanggotaan)
- `BETWEEN`(pemeriksaan jangkauan)

Operator logika

- `AND`
- `OR`
- `NOT`

[KELOMPOK BERDASARKAN properti]

Mengagregat hasil yang ditetapkan ke dalam kelompok baris dengan nilai yang cocok untuk properti yang diberikan.

Klausul GROUP BY berlaku untuk agregasi.

[PESANAN BERDASARKAN PROPERTI [ASC | DESC] [, properti [ASC | DESC]...]]

Mengurutkan hasil yang ditetapkan oleh satu atau lebih output`properties`.

Ketika klausa berisi beberapa properti, kumpulan hasil diurutkan menurut yang pertama`property`, lalu menurut yang kedua `property` untuk baris yang memiliki nilai yang cocok untuk properti pertama, dan seterusnya.

Contoh

```
SELECT resourceId WHERE resourceType='AWS::EC2::Instance'
```

```
SELECT configuration.complianceType, COUNT(*) WHERE resourceType =
 'AWS::Config::ResourceCompliance' GROUP BY configuration.complianceType
```

Kueri Menggunakan Editor Kueri SQL untuk AWS Config (Konsol)

Memperkenalkan fitur pratinjau untuk kueri lanjutan yang memungkinkan Anda menggunakan kemampuan kecerdasan buatan generatif (AI generatif) untuk memasukkan petunjuk dalam bahasa Inggris biasa dan mengubahnya menjadi format kueri. ready-to-use Untuk informasi selengkapnya, lihat Pemroses kueri bahasa alami untuk kueri lanjutan.

Anda dapat menggunakan kueri AWS sampel atau Anda dapat membuat kueri Anda sendiri yang disebut sebagai kueri kustom.

Pertimbangan

Prasyarat

Jika Anda menggunakan salah satu kebijakan AWS terkelola berikut, Anda akan memiliki izin yang diperlukan untuk menjalankan dan menyimpan kueri: AWSServiceRoleForConfig(peran terkait layanan) atau onFigRole. AWS_C

Jika tidak, Anda harus memiliki izin yang disertakan dalam kebijakan AWSConfigUserAccess AWS terkelola.

Daftar properti yang dapat Anda kueri

Daftar properti yang diperbarui dan tipe datanya tersedia di GitHub.

Kueri dan agregator tingkat lanjut

Untuk menjalankan kueri pada agregator, buat agregator. Untuk informasi selengkapnya, lihat Membuat Agregator untuk AWS Config.

Jika Anda sudah menyiapkan agregator, dalam lingkup kueri, pilih agregator untuk menjalankan kueri lanjutan pada agregator tersebut. Saat Anda memilih agregator, pertimbangkan untuk menambahkan Akun AWS ID dan AWS Wilayah dalam pernyataan kueri untuk melihat informasi tersebut dalam hasil.

Gunakan AWS Contoh Query

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.

2. Pilih Kueri lanjutan dari navigasi kiri untuk menanyakan konfigurasi sumber daya Anda untuk satu akun dan Wilayah atau untuk beberapa akun dan Wilayah.
3. Pada halaman Kueri lanjutan, pilih kueri yang sesuai dari daftar kueri. Anda dapat memfilter daftar kueri baik berdasarkan nama, deskripsi, pembuat, atau tag. Untuk memfilter AWS kueri, pilih Creator, dan masukkan AWS. Kueri yang Anda pilih ditampilkan di editor kueri SQL. Anda dapat mengedit kueri yang dipilih agar sesuai dengan kebutuhan Anda.
4. Untuk menyimpan kueri ini ke kueri baru, pilih Simpan Sebagai.
   - Di bidang Nama Kueri, perbarui nama kueri.
   - Di bidang Deskripsi, perbarui deskripsi kueri.
   - Masukkan hingga 50 tag unik untuk kueri ini.
   - Pilih Simpan.
5. Pilih Jalankan. Hasil kueri ditampilkan dalam tabel di bawah editor kueri.
6. Pilih Ekspor untuk mengekspor hasil kueri dalam format CSV atau JSON.

Buat kueri kustom Anda

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Pilih Kueri lanjutan dari navigasi kiri untuk menanyakan konfigurasi sumber daya Anda untuk satu akun dan Wilayah atau untuk beberapa akun dan Wilayah.
3. Untuk membuat kueri kustom Anda, pilih Kueri baru.

   Untuk melihat atau mengedit kueri kustom, filter kueri baik dengan nama, deskripsi, pembuat atau tag. Untuk memfilter kueri kustom, pilih Creater dan masukkan Custom.
4. Pada halaman Editor kueri, buat kueri Anda sendiri untuk akun dan Wilayah ini. Anda juga dapat memilih agregator yang sesuai untuk membuat kueri untuk beberapa akun dan Wilayah.
5. Edit jika Anda ingin membuat perubahan pada kueri ini. Pilih Simpan Kueri untuk menyimpan kueri ini.
   - Di bidang Nama Kueri, perbarui nama kueri.
   - Di bidang Deskripsi, perbarui deskripsi kueri.
   - Masukkan hingga 50 tag unik untuk kueri ini.
   - Pilih Simpan.

6. Pilih Jalankan. Hasil kueri ditampilkan dalam tabel di bawah editor kueri.
7. Pilih Ekspor untuk mengekspor hasil kueri dalam format CSV atau JSON.

Query Menggunakan SQL Query Editor untuk AWS Config ()AWS CLI

AWS CLI Ini adalah alat terpadu untuk mengelola AWS layanan Anda. Dengan hanya satu alat untuk mengunduh dan mengkonfigurasi, Anda dapat mengontrol beberapa AWS layanan dari baris perintah dan menggunakan skrip untuk mengotomatiskannya. Untuk informasi selengkapnya tentang AWS CLI dan untuk petunjuk tentang cara menginstal AWS CLI alat, lihat berikut ini di Panduan AWS Command Line Interface Pengguna.

- AWS Command Line Interface Panduan Pengguna
- Mempersiapkan AWS Command Line Interface

Jika perlu, masukkan `aws configure` untuk mengkonfigurasi AWS CLI untuk menggunakan AWS Wilayah di mana kueri lanjutan tersedia.

Pertimbangan

Prasyarat

Jika Anda menggunakan salah satu kebijakan AWS terkelola berikut, Anda akan memiliki izin yang diperlukan untuk menjalankan dan menyimpan kueri: AWSServiceRoleForConfig(peran terkait layanan) atau onFigRole. AWS_C

Jika tidak, Anda harus memiliki izin yang disertakan dalam kebijakan AWSConfigUserAccess AWS terkelola.

Daftar properti yang dapat Anda kueri

Daftar properti yang diperbarui dan tipe datanya tersedia di GitHub.

Kueri dan agregator tingkat lanjut

Untuk menjalankan kueri pada agregator, buat agregator. Untuk informasi selengkapnya, lihat Membuat Agregator untuk AWS Config.

Jika Anda sudah menyiapkan agregator, dalam lingkup kueri, pilih agregator untuk menjalankan kueri lanjutan pada agregator tersebut. Saat Anda memilih agregator, pertimbangkan untuk menambahkan Akun AWS ID dan AWS Wilayah dalam pernyataan kueri untuk melihat informasi tersebut dalam hasil.

Data Konfigurasi Sumber Daya Kueri

Untuk menanyakan data konfigurasi sumber daya Anda menggunakan editor kueri (AWS CLI) untuk satu akun dan Wilayah

1. Buka jendela command prompt atau terminal.
2. Masukkan perintah berikut untuk menanyakan data konfigurasi sumber daya Anda.

```
aws configservice select-resource-config --expression "SELECT resourceId WHERE
 resourceType='AWS::EC2::Instance'"
```

Bergantung pada kueri Anda, outputnya terlihat seperti berikut ini.

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}"
    ]
}
```

Untuk menanyakan data konfigurasi sumber daya Anda menggunakan editor kueri (AWS CLI) untuk beberapa akun dan Wilayah

1. Buka jendela command prompt atau terminal.
2. Masukkan perintah berikut untuk menanyakan data konfigurasi sumber daya Anda.

```
aws configservice select-aggregate-resource-config --expression "SELECT resourceId
 WHERE resourceType='AWS::EC2::Instance'" --configuration-aggregator-name my-
aggregator
```

Bergantung pada kueri Anda, outputnya terlihat seperti berikut ini.

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}"
    ]
}
```

> **Note**
>
> Saat menggunakan`AWS::IAM::User`,, `AWS::IAM::Group``AWS::IAM::Role`, dan jenis `AWS::IAM::Policy` sumber daya dalam kueri lanjutan, gunakan`awsRegion = 'global'`.

Menyimpan Kueri

1. Buka jendela command prompt atau terminal.
2. Masukkan perintah berikut untuk menyimpan kueri.

```
aws configservice put-stored-query --stored-query "{\"QueryName\": \"cli-test\",
 \"Expression\": \"SELECT *\", \"Description\": \"cli test query\" }"
        --tags "[{ \"Key\": \"first-tag\", \"Value\": \"\" }, { \"Key\": \"second-
tag\", \"Value\": \"non-empty-tag-value\" }]"
```

3. Bergantung pada kueri Anda, outputnya terlihat seperti berikut ini.

```
{
    "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/
query-e65mijt4rmam5pab"
}
```

> **Note**
>
> `--tags`adalah opsional. Ketika Anda melewati tag, tag yang disimpan tidak akan dikembalikan oleh salah satu `list-stored-queries` atau`get-stored-query`. Anda harus menggunakan `list-tag-for-resources` untuk mengambil tag terkait untuk kueri yang disimpan.
> `--description`bersifat opsional saat membuat atau memperbarui kueri.

Lihat semua Kueri Tersimpan

1. Masukkan perintah berikut untuk melihat daftar semua kueri yang disimpan.

```
aws configservice list-stored-queries
```

2. Bergantung pada kueri Anda, outputnya terlihat seperti berikut ini.

```
{
    "StoredQueryMetadata": [
        {
            "QueryId": "query-e65mijt4rmam5pab",
```

```
            "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-
test/query-e65mijt4rmam5pab",
            "QueryName": "cli-test"
        },
        {
            "QueryId": "query-rltwlewlqfivadxq",
            "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-
test-2/query-rltwlewlqfivadxq",
            "QueryName": "cli-test-2",
            "Description": "cli test query"
        }
    ]
}
}
```

Dapatkan Detail Kueri Tersimpan

1. Masukkan perintah berikut untuk mendapatkan detail kueri tersimpan tertentu.

```
aws configservice get-stored-query --query-name cli-test
```

2. Bergantung pada kueri Anda, outputnya terlihat seperti berikut ini.

```
{
    "StoredQuery": {
        "QueryId": "query-e65mijt4rmam5pab",
        "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/
query-e65mijt4rmam5pab",
        "QueryName": "cli-test",
        "Description": "cli test query",
        "Expression": "SELECT *"
    }
}
```

Hapus Kueri Tersimpan

- Masukkan perintah berikut untuk menghapus kueri tersimpan Anda.

```
aws configservice delete-stored-query --query-name cli-test
```

Jika berhasil, perintah berjalan tanpa output tambahan.

Prosesor kueri bahasa alami untuk kueri AWS Config tingkat lanjut

Prosesor kueri bahasa alami untuk kueri lanjutan ada dalam rilis pratinjau untuk AWS Config dan dapat berubah sewaktu-waktu.

Prosesor kueri bahasa alami untuk kueri lanjutan menggunakan Amazon Bedrock, teknologi kecerdasan buatan generatif (AI generatif) yang memungkinkan Anda memasukkan petunjuk dalam bahasa Inggris biasa dan mengubahnya menjadi format kueri. ready-to-use Dengan prosesor kueri bahasa alami, Anda dapat melakukan kueri Akun AWS atau di seluruh AWS organisasi.

Prompt bisa berupa pertanyaan atau pernyataan. Misalnya, Anda dapat memasukkan petunjuk seperti “Penyeimbang beban mana yang dibuat setelah 1 Januari 2024?” dan “Buat daftar semua fungsi lambda saya yang menjalankan node js 16.”

Pertimbangan

Prosesor kueri bahasa alami tidak dapat melakukan tindakan berikut:

- Hasilkan kueri dari bahasa selain bahasa Inggris.
- Hasilkan kueri dari prompt yang tidak berhubungan dengan kueri lanjutan.
- Hasilkan kueri dari prompt dengan lebih dari 1000 karakter.
- Hasilkan kueri dari koreksi tindak lanjut atau dari sesi sebelumnya.
- Jelaskan kode yang telah dihasilkan.

Kueri menggunakan prosesor kueri bahasa alami

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Pilih Kueri lanjutan dari navigasi kiri untuk menanyakan konfigurasi sumber daya Anda untuk satu akun dan Wilayah atau untuk beberapa akun dan Wilayah.
3. Pada halaman Advanced queries, pilih New query untuk pergi ke Query editor.
   - (Opsional) Untuk menjalankan kueri pada agregator, buat agregator. Untuk informasi selengkapnya, lihat Membuat Agregator untuk AWS Config.

- Jika Anda sudah menyiapkan agregator, dalam lingkup kueri, pilih agregator untuk menjalankan kueri lanjutan pada agregator tersebut. Saat Anda memilih agregator, pertimbangkan untuk menambahkan Akun AWS ID dan AWS Wilayah dalam pernyataan kueri untuk melihat informasi tersebut dalam hasil.

4. Di editor Kueri, buka bagian prosesor kueri bahasa alami. Masukkan prompt dalam bahasa Inggris biasa, lalu pilih Hasilkan. Sebagai contoh, lihat Contoh prompt.
5. Setelah Anda membuat kueri, Anda dapat memilih Salin (secara fungsional setara dengan Ctrl +C) untuk menyalin kueri ke clipboard Anda, atau memilih Populasi ke editor. Jika diisi ke editor, Anda dapat mengedit kueri yang dihasilkan agar sesuai dengan kebutuhan Anda.
6. Untuk menyimpan kueri ini ke kueri baru, pilih Simpan Sebagai.
   - Di bidang Nama Kueri, perbarui nama kueri.
   - Di bidang Deskripsi, perbarui deskripsi kueri.
   - Masukkan hingga 50 tag unik untuk kueri ini.
   - Pilih Simpan.
7. Pilih Jalankan. Hasil query ditampilkan dalam tabel di bawah editor query.
8. Pilih Ekspor untuk mengekspor hasil kueri dalam format CSV atau JSON.

> **Note**
>
> Hasil kueri diberi paginasi. Saat Anda mengekspor, hingga 500 hasil diekspor. Anda juga dapat menggunakan APIs untuk mengambil semua hasil. Hasilnya diberi paginasi dan Anda dapat mengambil 100 hasil sekaligus.

Contoh petunjuk

Berikut ini adalah petunjuk dan menghasilkan kueri yang dapat Anda gunakan sebagai contoh.

Example: Penyeimbang beban apa yang dibuat setelah 1 Januari 2024?

Prompt: What load balancers were created after January 1, 2024?

Kueri yang dihasilkan:

```
SELECT
```

```
    resourceId,
    resourceType,
    resourceCreationTime
WHERE
    resourceType IN ('AWS::ElasticLoadBalancing::LoadBalancer',
 'AWS::ElasticLoadBalancingV2::LoadBalancer')
AND
    resourceCreationTime > '2024-01-01T00:00:00.0Z'
ORDER BY
    resourceCreationTime
DESC
```

Example: Manakah dari instance database RDS saya yang dapat diakses publik?

Prompt: Which of my RDS database instances are publicly accessible?

Kueri yang dihasilkan:

```
SELECT
    resourceId,
    resourceType,
    configuration.publiclyAccessible
WHERE
    resourceType = 'AWS::RDS::DBInstance'
AND
    configuration.publiclyAccessible = true
```

Example: Berapa banyak EC2 contoh yang dibuat dalam satu tahun terakhir?

Prompt: How many EC2 instances were created in last one year?

Kueri yang dihasilkan:

```
SELECT
    COUNT(*)
WHERE
    resourceType = 'AWS::EC2::Instance'
AND
    resourceCreationTime
BETWEEN
    '2023-05-10T16:56:25.000Z'
AND
```

```
    '2024-05-10T16:56:25.000Z'
```

Example: Berapa banyak EC2 contoh yang saya miliki di masing-masing? Akun AWS

Prompt: How many EC2 instances do I have in each of my Akun AWS?

Kueri yang dihasilkan:

```
SELECT
    accountId,
    COUNT(*)
WHERE
    resourceType = 'AWS::EC2::Instance'
GROUP BY
    accountId'
```

Example: Peran IAM mana yang memiliki kebijakan terkelola yang AdministratorAccess dilampirkan?

Prompt: Which IAM roles have the managed policy AdministratorAccess attached?

Kueri yang dihasilkan:

```
SELECT
    resourceId,
    resourceName,
    resourceType
WHERE
    resourceType = 'AWS::IAM::Role'
AND
    configuration.attachedManagedPolicies.policyName = 'AdministratorAccess'
```

Example: Volume EBS tanpa enkripsi

Prompt: EBS volumes without encryption

Kueri yang dihasilkan:

```
SELECT
    accountId
WHERE
    resourceType = 'AWS::EC2::Volume'
```

```
AND
    configuration.encrypted = false
```

Example: Dapatkan sumber daya yang tidak sesuai

Prompt: Get noncompliant resources

Kueri yang dihasilkan:

```
SELECT
    resourceId,
    resourceType
WHERE
    resourceType = 'AWS::Config::ResourceCompliance'
AND
    configuration.complianceType = 'NON_COMPLIANT'
```

Example: Buat daftar semua fungsi lambda saya yang menjalankan node js 16

Prompt: List all my lambda function that is running node js 16

Kueri yang dihasilkan:

```
SELECT
    accountId,
    resourceName
WHERE
    resourceType = 'AWS::Lambda::Function'
AND
    configuration.runtime = 'nodejs16.x'
```

Example: Sertifikat ACM apa yang kedaluwarsa 30 hari ke depan?

Prompt: What ACM certificates expire the next 30 days?

Kueri yang dihasilkan:

```
SELECT
    resourceId,
    configuration.domainName,
    configuration.notAfter
```

```
WHERE
    resourceType = 'AWS::ACM::Certificate'
AND
    configuration.notAfter
BETWEEN
    '2024-05-10 16:59:53'
AND
    '2024-06-10 16:59:53’
```

> **Note**
>
> Waktu dalam kueri yang dihasilkan tergantung pada waktu ketika Anda memasukkan prompt.

Memberikan umpan balik

Anda dapat memberikan umpan balik keseluruhan tentang pemroses kueri bahasa alami atau umpan balik tentang kueri tertentu yang dihasilkan.

Memberikan umpan balik pada prosesor kueri bahasa alami

Pilih tombol Berikan umpan balik yang muncul di atas prosesor kueri bahasa alami di sebelah kanan. Anda dapat memasukkan kepuasan atau ketidakpuasan Anda dan memberikan umpan balik tentang bagaimana AWS Config dapat membuat kueri bahasa alami lebih bermanfaat.

> **Note**
>
> Jangan mengungkapkan informasi pribadi, sensitif komersial, atau rahasia apa pun.

Memberikan umpan balik pada kueri yang dihasilkan tertentu

Anda dapat memberikan umpan balik Anda pada kueri yang dihasilkan dengan memilih tombol jempol ke atas atau jempol ke bawah yang muncul di bawah kueri yang dihasilkan.

Support Wilayah

Prosesor kueri bahasa alami didukung di Wilayah berikut.

Nama Wilayah	Wilayah	Titik Akhir	Protokol
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS

Contoh Query untuk AWS Config

Lihat contoh query berikut.

Query to list all EC2 instances with AMI ID ami-12345

Kueri:

```
SELECT
    resourceId,
    resourceType,
    configuration.instanceType,
    configuration.placement.tenancy,
    configuration.imageId,
    availabilityZone
WHERE
    resourceType = 'AWS::EC2::Instance'
AND
    configuration.imageId = 'ami-12345'
```

Hasil:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
```

```
                "Name": "resourceType"
            },
            {
                "Name": "configuration.instanceType"
            },
            {
                "Name": "configuration.placement.tenancy"
            },
            {
                "Name": "configuration.imageId"
            },
            {
                "Name": "availabilityZone"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2a\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t1.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2a\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}"
    ]
}
```

Query for count of resources grouped by their AWS Config rules compliance status

Kueri:

```
SELECT
    configuration.complianceType,
    COUNT(*)
WHERE
    resourceType = 'AWS::Config::ResourceCompliance'
GROUP BY
    configuration.complianceType
```

Hasil:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "configuration.complianceType"
            },
            {
                "Name": "COUNT(*)"
            }
        ]
    },
    "Results": [
        "{\"COUNT(*)\":163,\"configuration\":{\"complianceType\":\"NON_COMPLIANT
\"}}",
        "{\"COUNT(*)\":2,\"configuration\":{\"complianceType\":\"COMPLIANT\"}}"
    ]
}
```

Query for the compliance status of AWS Conformance packs

Kueri:

```
SELECT
    resourceId,
    resourceName,
    resourceType,
    configuration.complianceType
WHERE
    resourceType = 'AWS::Config::ConformancePackCompliance'
```

Hasil:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "resourceName"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.complianceType"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"COMPLIANT\"},\"resourceName\":\"MyConformancePack1\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}",
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"NON_COMPLIANT\"},\"resourceName\":\"MyConformancePack2\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}",
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"NON_COMPLIANT\"},\"resourceName\":\"MyConformancePack3\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}"
    ]
}
```

Query to get counts of AWS resources grouped by account ID

Kueri:

```
aws configservice select-aggregate-resource-config --expression "SELECT COUNT(*),
 accountId group by accountId" --configuration-aggregator-name my-aggregator
```

Hasil:

```
{
    "Results": [
        "{\"COUNT(*)\":2407,\"accountId\":\"accountId\"}",
        "{\"COUNT(*)\":726,\"accountId\":\"accountId\"}"
```

```
    ],
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "COUNT(*)"
            },
            {
                "Name": "accountId"
            }
        ]
    }
}
```

Query to list all EC2 volumes that are not in use

Kueri:

```
SELECT
    resourceId,
    accountId,
    awsRegion,
    resourceType,
    configuration.volumeType,
    configuration.size,
    resourceCreationTime,
    tags,
    configuration.encrypted,
    configuration.availabilityZone,
    configuration.state.value
WHERE
    resourceType = 'AWS::EC2::Volume'
AND
    configuration.state.value = 'available'
```

Hasil:

```
{
    "Results": [
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0174de9c962f6581c\",
\"awsRegion\":\"us-west-2\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
```

```
\"us-west-2a\"},\"resourceCreationTime\":\"2020-02-21T07:39:43.771Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}",
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0cbeb652a74af2f8f\",
\"awsRegion\":\"us-east-1\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"us-east-1a\"},\"resourceCreationTime\":\"2020-02-21T07:28:40.639Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}"
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0a49952d528ec8ba2\",
\"awsRegion\":\"ap-south-1\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"ap-south-1a\"},\"resourceCreationTime\":\"2020-02-21T07:39:31.800Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}",
    ],
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "accountId"
            },
            {
                "Name": "awsRegion"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.volumeType"
            },
            {
                "Name": "configuration.size"
            },
            {
                "Name": "resourceCreationTime"
            },
            {
                "Name": "tags"
            },
            {
                "Name": "configuration.encrypted"
            },
            {
                "Name": "configuration.availabilityZone"
```

```
            },
            {
                "Name": "configuration.state.value"
            }
        ]
    }
}
```

Contoh Pertanyaan Hubungan untuk AWS Config

Lihat contoh query hubungan berikut.

Find EIPs related to an EC2 instance

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::EIP'
    AND relationships.resourceId = 'i-abcd1234'
```

Find EIPs related to an EC2 network interface

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::EIP'
    AND relationships.resourceId = 'eni-abcd1234'
```

Find EC2 instances and network interfaces related to a security group

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::NetworkInterface')
    AND relationships.resourceId = 'sg-abcd1234'
```

ATAU

```
SELECT
    resourceId
```

```
WHERE
    resourceType = 'AWS::EC2::Instance'
    AND relationships.resourceId = 'sg-abcd1234'

SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::NetworkInterface'
    AND relationships.resourceId = 'sg-abcd1234'
```

Find EC2 instances, network ACLs, network interfaces and route tables related to a subnet

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::NetworkACL',
 'AWS::EC2::NetworkInterface', 'AWS::EC2::RouteTable')
    AND relationships.resourceId = 'subnet-abcd1234'
```

Find EC2 instances, internet gateways, network ACLs, network interfaces, route tables, subnets and security groups related to a VPC

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::InternetGateway',
 'AWS::EC2::NetworkACL', 'AWS::EC2::NetworkInterface', 'AWS::EC2::RouteTable',
 'AWS::EC2::Subnet', 'AWS::EC2::SecurityGroup')
    AND relationships.resourceId = 'vpc-abcd1234'
```

Find EC2 route tables related to a VPN gateway

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::RouteTable'
    AND relationships.resourceId = 'vgw-abcd1234'
```

Batasan

> **Note**
>
> Kueri lanjutan tidak mendukung sumber daya kueri yang belum dikonfigurasi untuk direkam oleh perekam konfigurasi. AWS Config membuat Item Konfigurasi (CIs) dengan `ResourceNotRecorded` `configurationItemStatus` ketika sumber daya telah ditemukan tetapi tidak dikonfigurasi untuk direkam oleh perekam konfigurasi. Sementara agregator akan menggabungkan ini CIs, kueri lanjutan tidak mendukung kueri dengan. CIs `ResourceNotRecorded` Perbarui pengaturan perekam Anda untuk mengaktifkan perekaman jenis sumber daya yang ingin Anda kueri.

Sebagai bagian dari SQL`SELECT`, sintaks kueri memiliki batasan berikut:

- Tidak ada dukungan untuk`ALL`,`AS`,`DISTINCT`,`FROM`,`HAVING`,`JOIN`, dan `UNION` kata kunci dalam kueri. `NULL`kueri nilai tidak didukung.
- Tidak ada dukungan untuk `CASE` pernyataan kompleks untuk membuat bidang prioritas langsung dalam kueri.
- Tidak ada dukungan untuk kueri pada sumber daya pihak ketiga. Sumber daya pihak ketiga yang diambil menggunakan kueri lanjutan akan memiliki bidang konfigurasi yang ditetapkan sebagai. `NULL`
- Tidak ada dukungan untuk struktur bersarang (seperti tag) untuk dibongkar dengan kueri SQL.
- Tidak ada dukungan untuk menanyakan sumber daya yang dihapus. Untuk menemukan sumber daya yang dihapus, lihat Mencari Sumber Daya yang Ditemukan oleh AWS Config.
- Singkatan `SELECT` semua kolom (yaitu`SELECT *`) hanya memilih properti skalar tingkat atas dari CI. Sifat skalar yang dikembalikan adalah `accountIdawsRegion`,,`arn`,`availabilityZone`,`configurationItemCaptureTime`,`resourceCre` `resourceNameresourceType`, dan`version`.
- Batasan wildcard:
  - Wildcard hanya didukung untuk nilai properti dan bukan untuk kunci properti (misalnya, `...WHERE someKey LIKE 'someValue%'` didukung tetapi tidak `...WHERE 'someKey%' LIKE 'someValue%'` didukung).

- Support hanya untuk wildcard akhiran (misalnya, `...LIKE 'AWS::EC2::%'` dan `...LIKE 'AWS::EC2::_'` didukung tetapi `...LIKE '%::EC2::Instance'` dan tidak `...LIKE '_::EC2::Instance'` didukung).
- Pencocokan wildcard harus memiliki panjang minimal tiga karakter (misalnya, `...LIKE 'ab%'` dan tidak `...LIKE 'ab_'` diperbolehkan tetapi `...LIKE 'abc%'` diizinkan). `...LIKE 'abc_'`

> **Note**
>
> "_" (garis bawah tunggal) juga diperlakukan sebagai wildcard.

- Batasan agregasi:
  - Fungsi agregat hanya dapat menerima satu argumen atau properti.
  - Fungsi agregat tidak dapat mengambil fungsi lain sebagai argumen.
  - `GROUP BY`dengan `ORDER BY` klausa referensi fungsi agregat mungkin hanya berisi satu properti.
  - Untuk semua `GROUP BY` klausa agregasi lainnya mungkin berisi hingga tiga properti.
  - Pagination didukung untuk semua kueri agregat kecuali ketika `ORDER BY` klausa memiliki fungsi agregat. Misalnya, `GROUP BY X, ORDER BY Y` tidak berfungsi jika Y merupakan fungsi agregat.
  - Tidak ada dukungan untuk `HAVING` klausa dalam agregasi.
- Batasan pengenal yang tidak cocok:

  Pengidentifikasi yang tidak cocok adalah properti yang memiliki ejaan yang sama tetapi kasus yang berbeda (huruf besar dan kecil). Kueri lanjutan tidak mendukung kueri pemrosesan yang berisi pengidentifikasi yang tidak cocok. Misalnya:

  - Dua properti yang memiliki ejaan yang sama persis tetapi dengan casing yang berbeda (`configuration.dbclusterIdentifierdanconfiguration.dBClusterIdentifier`).
  - Dua properti di mana satu properti adalah bagian dari yang lain, dan mereka memiliki casing yang berbeda (`configuration.ipAddressdanconfiguration.ipaddressPermissions`).

Perilaku notation/IP rentang CIDR untuk kueri lanjutan

Notasi CIDR dikonversi ke rentang IP untuk pencarian.

Ini berarti bahwa "=" dan "BETWEEN" mencari rentang apa pun yang mencakup IP yang disediakan, bukan yang tepat.

Untuk mencari rentang IP yang tepat, Anda perlu menambahkan kondisi tambahan untuk mengecualikan IPs di luar jangkauan.

Example Mencari blok CIDR yang tepat 10.0.0.0/24

```
SELECT * WHERE resourceType = 'AWS::EC2::SecurityGroup'
  AND configuration.ipPermissions.ipRanges BETWEEN '10.0.0.0'
  AND '10.0.0.255'
  AND NOT configuration.ipPermissions.ipRanges < '10.0.0.0'
  AND NOT configuration.ipPermissions.ipRanges > '10.0.0.255'
```

Example Mencari alamat IP yang tepat 192.168.0.2/32

```
SELECT * WHERE resourceType = 'AWS::EC2::SecurityGroup'
  AND configuration.ipPermissions.ipRanges = '192.168.0.2'
  AND NOT configuration.ipPermissions.ipRanges > '192.168.0.2'
  AND NOT configuration.ipPermissions.ipRanges < '192.168.0.2'
```

Beberapa properti dalam perilaku array untuk kueri lanjutan

Saat melakukan kueri terhadap beberapa properti dalam array objek, kecocokan dihitung terhadap semua elemen array.

Misalnya, untuk sumber daya R dengan aturan A dan B, sumber daya sesuai dengan aturan A tetapi tidak sesuai dengan aturan B. Sumber daya R disimpan sebagai:

```
{
    configRuleList: [
        {
            configRuleName: 'A', complianceType: 'compliant'
        },
        {
            configRuleName: 'B', complianceType: 'non_compliant'
        }
    ]
}
```

R akan dikembalikan oleh kueri ini:

```
SELECT configuration WHERE configuration.configRuleList.complianceType =
 'non_compliant'
AND configuration.configRuleList.configRuleName = 'A'
```

Kondisi pertama `configuration.configRuleList.complianceType = 'non_compliant'` diterapkan ke SEMUA elemen di R.configRuleList, karena R memiliki aturan (aturan B) dengan complianceType = 'non_compliant', kondisi dievaluasi sebagai true.

Kondisi kedua `configuration.configRuleList.configRuleName` diterapkan pada SEMUA elemen di R.configRuleList, karena R memiliki aturan (aturan A) dengan configRuleName = 'A', kondisi dievaluasi sebagai benar. Karena kedua kondisi tersebut benar, R akan dikembalikan.

Support Wilayah

Kueri lanjutan didukung di Wilayah berikut:

Nama Wilayah	Wilayah	Titik Akhir	Protokol
AS Timur (Ohio)	us–east-2	config.us-east-2.amazonaws.com	HTTPS
AS Timur (Virginia Utara)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
AS Barat (Californ ia Utara)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
AS Barat (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
Afrika (Cape Town)	af-south-1	config.af-south-1.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Asia Pasifik (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asia Pasifik (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asia Pasifik (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asia Pasifik (Malaysia)	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS
Asia Pasifik (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia Pasifik (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pasifik (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia Pasifik (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Asia Pasifik (Singapura)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pasifik (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pasifik (Taipei)	ap-timur-2	config.ap-east-2.amazonaws.com	HTTPS
Asia Pasifik (Thailand)	ap-tenggara 7	config.ap-southeast-7.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Kanada (Pusat)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Kanada Barat (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Eropa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Eropa (Irlandia)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Eropa (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Eropa (Milan)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Eropa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Eropa (Spanyol)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Eropa (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Eropa (Zürich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Meksiko (Tengah)	mx-pusat-1	config.mx-central-1.amazonaws.com	HTTPS
Timur Tengah (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Timur Tengah (UAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol	
Amerika Selatan (Sao Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS	
AWS GovCloud (AS-Timur)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS	
AWS GovCloud (AS-Barat)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS	

Menghapus Data AWS Config

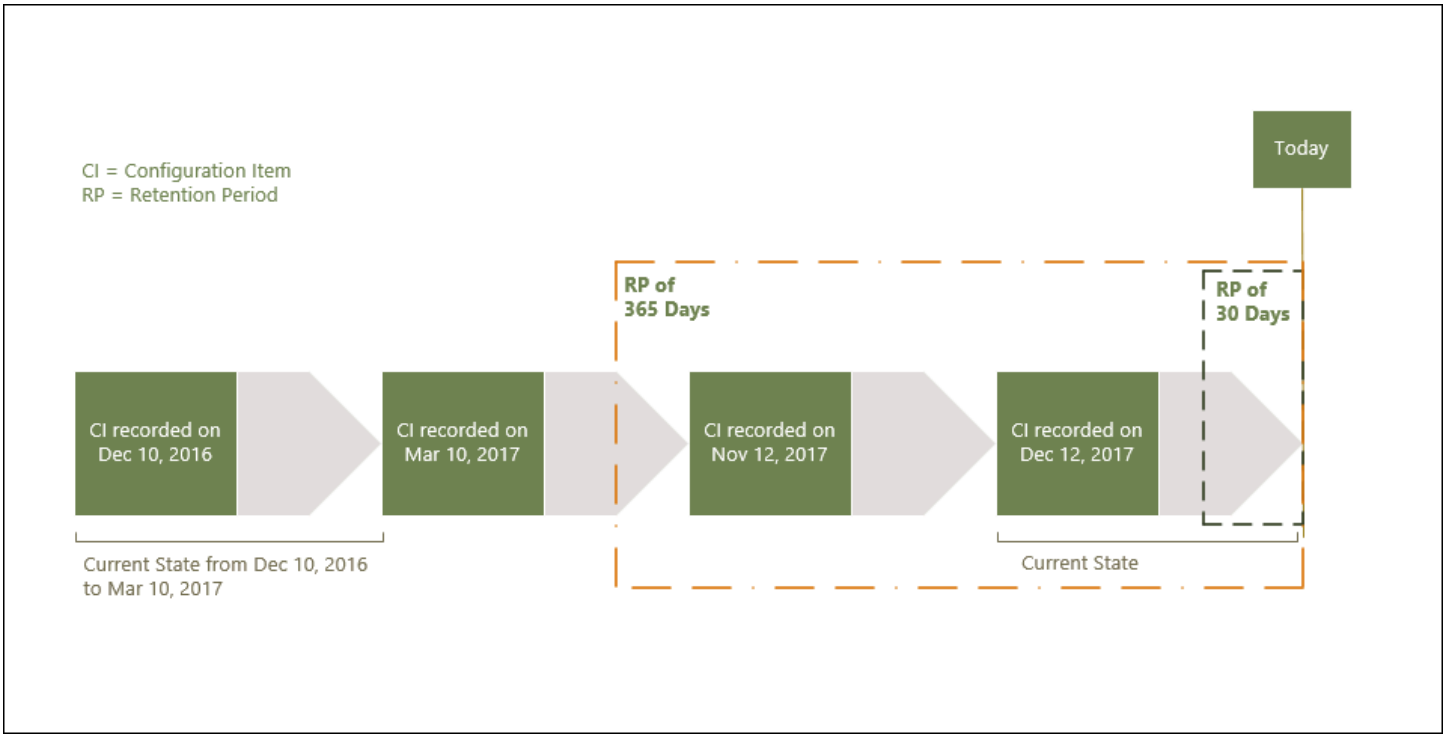
> **Note**
>
> Saat AWS Config menggunakan Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) dan Amazon Simple Notification Service (Amazon SNS) untuk mengirim snapshot konfigurasi dan file AWS Config riwayat konfigurasi, memiliki kebijakan penyimpanan dan penyimpanan data sendiri. Informasi di halaman ini khusus untuk AWS Config. Amazon S3 dan Amazon SNS memiliki kebijakan penyimpanan dan penyimpanan data terpisah mereka sendiri.

AWS Config memungkinkan Anda untuk menghapus data Anda dengan menentukan periode retensi untuk Anda`ConfigurationItems`. Saat Anda menentukan periode retensi, AWS Config pertahankan periode Anda `ConfigurationItems` untuk periode yang ditentukan. Anda dapat memilih periode antara minimal 30 hari dan maksimal 7 tahun (2557 hari). AWS Config menghapus data yang lebih lama dari periode retensi yang Anda tentukan. Jika Anda tidak menentukan periode retensi, AWS Config terus simpan `ConfigurationItems` untuk periode default 7 tahun (2557 hari). Saat perekaman dinyalakan, keadaan sumber daya saat ini adalah saat a `ConfigurationItem` direkam dan sampai perubahan berikutnya (baru`ConfigurationItem`) direkam.

Untuk memahami perilaku periode retensi, mari kita lihat timeline.

- Saat perekaman diaktifkan, status sumber daya saat ini selalu ada dan tidak dapat dihapus terlepas dari tanggal `ConfigurationItem` perekaman.
- Saat AWS Config merekam baru`ConfigurationItems`, yang sebelumnya `ConfigurationItems` dihapus tergantung pada periode retensi yang ditentukan.

Dalam timeline berikut, AWS Config catat `ConfigurationItems` pada tanggal-tanggal berikut. Untuk tujuan timeline ini, hari ini direpresentasikan sebagai 24 Mei 2018.



Tabel berikut menjelaskan mana yang `ConfigurationItems` ditampilkan pada AWS Config timeline berdasarkan periode retensi yang dipilih.

Periode Retensi	Item Konfigurasi ditampilkan di timeline	Penjelasan
30 hari	12 Desember 2017	Keadaan sumber daya saat ini dimulai dari 12 Desember 2017 ketika `ConfigurationItem` direkam dan berlaku hingga hari ini (24 Mei 2018). Saat perekaman dihidupkan, keadaan saat ini selalu ada.
365 hari	12 Desember 2017; 12 November 2017, dan 10 Maret 2017	Periode retensi menunjukkan keadaan saat ini 12 Desember 2017 dan sebelumnya 12 `ConfigurationItems` November 2017 dan 10 Maret 2017.

Periode Retensi	Item Konfigurasi ditampilkan di timeline	Penjelasan
		`ConfigurationItem` Untuk 10 Maret 2017 ditampilkan pada timeline karena status konfigurasi tersebut mewakili status saat ini 365 hari yang lalu.

Setelah Anda menentukan periode retensi, AWS Config APIs tidak lagi kembali `ConfigurationItems` yang mewakili status yang lebih lama dari periode retensi yang ditentukan.

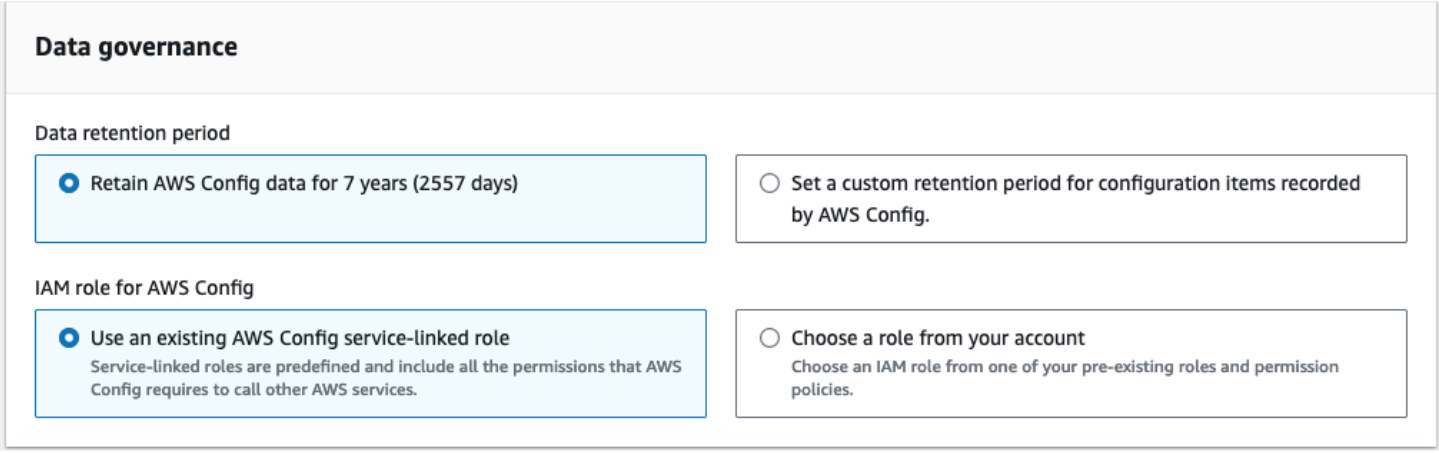
> **Note**
>
> - AWS Config tidak dapat merekam Anda `ConfigurationItems` jika rekaman dimatikan.
> - AWS Config tidak dapat merekam `ConfigurationItems` jika peran IAM Anda tidak memiliki izin yang memadai. Untuk informasi selengkapnya, lihat Izin untuk Peran IAM yang Ditetapkan. AWS Config

Mengatur Periode Retensi Data di AWS Management Console

Dalam AWS Management Console, jika Anda tidak memilih periode penyimpanan data, periode default adalah 7 tahun atau 2557 hari.

Untuk mengatur periode penyimpanan data kustom untuk item konfigurasi, pilih kotak centang. Anda dapat memilih 1 tahun, 3 tahun, 5 tahun, atau periode kustom. Untuk periode kustom, masukkan jumlah hari antara 30 dan 2557 hari.

Gambar berikut menampilkan tempat Anda dapat mengatur periode retensi data di Tata Kelola Data. Anda dapat mengakses Tata Kelola Data di halaman Edit Pengaturan dari AWS Config konsol dengan memilih Pengaturan di bilah navigasi kiri, lalu memilih Edit.


Data governance
Data retention period
Retain AWS Config data for 7 years (2557 days)
Set a custom retention period for configuration items recorded by AWS Config.
IAM role for AWS Config
Use an existing AWS Config service-linked role
Service-linked roles are predefined and include all the permissions that AWS Config requires to call other AWS services.
Choose a role from your account
Choose an IAM role from one of your pre-existing roles and permission policies.

Keamanan di AWS Config

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan dari cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program AWS Kepatuhan Program AWS Kepatuhan . Untuk mempelajari tentang program kepatuhan yang berlaku AWS Config, lihat AWS layanan dalam Layanan Cakupan oleh Program AWS Kepatuhan .
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan AWS Config. Topik berikut menunjukkan cara mengonfigurasi AWS Config untuk memenuhi tujuan keamanan dan kepatuhan Anda.

Topik

- Perlindungan Data di AWS Config
- Identity and Access Management untuk AWS Config
- Respon Insiden di AWS Config
- Validasi Kepatuhan untuk AWS Config
- Ketahanan di AWS Config
- Keamanan Infrastruktur di AWS Config
- Pencegahan "confused deputy" lintas layanan
- Praktik Terbaik Keamanan untuk AWS Config

Perlindungan Data di AWS Config

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di AWS Config. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam Pertanyaan Umum Privasi Data. Lihat informasi tentang perlindungan data di Eropa di pos blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan AWS .

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensil dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat Bekerja dengan CloudTrail jejak di AWS CloudTrail Panduan Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-3.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan AWS Config atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau. AWS SDKs Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan

atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Enkripsi Data Saat Tidak Digunakan

Data dienkripsi saat istirahat menggunakan enkripsi sisi server transparan. Hal ini membantu mengurangi beban operasional dan kompleksitas yang terlibat dalam melindungi data sensitif. Dengan enkripsi saat istirahat, Anda dapat membangun aplikasi yang sensitif terhadap keamanan yang memenuhi persyaratan kepatuhan enkripsi dan peraturan.

Enkripsi Data dalam Transit

Data yang dikumpulkan dan diakses oleh AWS Config secara eksklusif melalui saluran yang dilindungi Transport Layer Security (TLS).

Identity and Access Management untuk AWS Config

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya. AWS Config IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Audiens
- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan
- Bagaimana AWS Config bekerja dengan IAM
- Contoh kebijakan berbasis identitas untuk AWS Config
- AWS kebijakan terkelola untuk AWS Config
- Izin untuk Peran IAM Ditugaskan AWS Config
- Memperbarui Peran IAM untuk perekam konfigurasi terkelola pelanggan
- Izin untuk Bucket Amazon S3 untuk AWS Config Saluran Pengiriman
- Izin untuk Kunci KMS untuk Saluran Pengiriman AWS Config
- Izin untuk Topik Amazon SNS

- Memecahkan masalah AWS Config identitas dan akses
- Menggunakan Peran Tertaut Layanan untuk AWS Config

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan. AWS Config

Pengguna layanan — Jika Anda menggunakan AWS Config layanan untuk melakukan pekerjaan Anda, maka administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak AWS Config fitur untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara mengelola akses dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di AWS Config, lihat Memecahkan masalah AWS Config identitas dan akses.

Administrator layanan — Jika Anda bertanggung jawab atas AWS Config sumber daya di perusahaan Anda, Anda mungkin memiliki akses penuh ke AWS Config. Tugas Anda adalah menentukan AWS Config fitur dan sumber daya mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasar IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM AWS Config, lihatBagaimana AWS Config bekerja dengan IAM.

Administrator IAM – Jika Anda adalah administrator IAM, Anda mungkin ingin belajar dengan lebih detail tentang cara Anda menulis kebijakan untuk mengelola akses ke AWS Config. Untuk melihat contoh kebijakan AWS Config berbasis identitas yang dapat Anda gunakan di IAM, lihat. Contoh kebijakan berbasis identitas untuk AWS Config

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensyal yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda

sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Guna mengetahui informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat AWS Signature Version 4 untuk permintaan API dalam Panduan Pengguna IAM.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat Autentikasi multi-faktor dalam Panduan Pengguna AWS IAM Identity Center dan Autentikasi multi-faktor AWS di IAM dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensil yang disediakan melalui sumber identitas. Ketika

identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensyal sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat Apakah itu Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, kami merekomendasikan untuk mengandalkan kredensial sementara, bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi kunci akses. Untuk informasi selengkapnya, lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

Grup IAM adalah identitas yang menentukan sekumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat meminta kelompok untuk menyebutkan IAMAdmins dan memberikan izin kepada grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat Kasus penggunaan untuk pengguna IAM dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Untuk mengambil peran IAM sementara AWS Management Console, Anda dapat beralih dari pengguna ke peran IAM (konsol). Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat Metode untuk mengambil peran dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Buat peran untuk penyedia identitas pihak ketiga dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (prinsipal tepercaya) di akun lain untuk mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Misalnya, saat Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.
  - Peran layanan – Peran layanan adalah peran IAM yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.

- Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI atau AWS permintaan API. Ini lebih baik untuk menyimpan kunci akses dalam EC2 instance. Untuk menetapkan AWS peran ke EC2 instance dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instance berisi peran dan memungkinkan program yang berjalan pada EC2 instance untuk mendapatkan kredensi sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon di Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasinya. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat dilampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan yang dikelola atau kebijakan inline, lihat Pilih antara kebijakan yang dikelola dan kebijakan inline dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Daftar kontrol akses (ACLs)

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung. ACLs Untuk mempelajari selengkapnya ACLs, lihat Ringkasan daftar kontrol akses (ACL) di Panduan Pengembang Layanan Penyimpanan Sederhana Amazon.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas IAM (pengguna IAM atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCPs) — SCPs adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di. AWS Organizations AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS Untuk informasi selengkapnya tentang Organizations dan SCPs, lihat Kebijakan kontrol layanan di Panduan AWS Organizations Pengguna.
- Kebijakan kontrol sumber daya (RCPs) — RCPs adalah kebijakan JSON yang dapat Anda gunakan untuk menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda tanpa memperbarui kebijakan IAM yang dilampirkan ke setiap sumber daya yang Anda miliki. RCP membatasi izin untuk sumber daya di akun anggota dan dapat memengaruhi izin efektif untuk identitas, termasuk Pengguna root akun AWS, terlepas dari apakah itu milik organisasi Anda. Untuk informasi selengkapnya tentang Organizations dan RCPs, termasuk daftar dukungan Layanan AWS tersebut RCPs, lihat Kebijakan kontrol sumber daya (RCPs) di Panduan AWS Organizations Pengguna.
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Bagaimana AWS Config bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses AWS Config, pelajari fitur IAM yang tersedia untuk digunakan. AWS Config

Fitur IAM yang dapat Anda gunakan dengan AWS Config

Fitur IAM	AWS Config dukungan
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
kunci-kunci persyaratan kebijakan (spesifik layanan)	Ya
ACLs	Tidak
ABAC (tanda dalam kebijakan)	Ya
Kredensial sementara	Ya
Sesi akses teruskan (FAS)	Ya
Peran layanan	Ya
Peran terkait layanan	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara AWS Config dan AWS layanan lain bekerja dengan sebagian besar fitur IAM, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Kebijakan berbasis identitas untuk AWS Config

Mendukung kebijakan berbasis identitas: Ya

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Contoh kebijakan berbasis identitas untuk AWS Config

Untuk melihat contoh kebijakan AWS Config berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk AWS Config

Kebijakan berbasis sumber daya dalam AWS Config

Mendukung kebijakan berbasis sumber daya: Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai prinsipal dalam kebijakan berbasis sumber daya. Menambahkan prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, administrator IAM di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke principal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

Tindakan kebijakan untuk AWS Config

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, misalnya tindakan hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar AWS Config tindakan, lihat Tindakan yang ditentukan oleh AWS Config dalam Referensi Otorisasi Layanan.

Tindakan kebijakan AWS Config menggunakan awalan berikut sebelum tindakan:

```
config
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

```
"Action": [
      "config:action1",
      "config:action2"
         ]
```

Anda juga dapat menentukan beberapa tindakan menggunakan wildcard (*). Sebagai contoh, untuk menentukan semua tindakan yang dimulai dengan kata `Describe`, sertakan tindakan berikut:

```
"Action": "config:Describe*"
```

Untuk melihat contoh kebijakan AWS Config berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk AWS Config

Sumber daya kebijakan untuk AWS Config

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Untuk melihat daftar jenis sumber daya dan jenis AWS Config sumber daya ARNs, lihat Sumber daya yang ditentukan oleh AWS Config dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan yang dapat menentukan ARN setiap sumber daya, lihat Tindakan yang ditentukan oleh AWS Config.

Untuk melihat contoh kebijakan AWS Config berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk AWS Config

Kunci kondisi kebijakan untuk AWS Config

Mendukung kunci kondisi kebijakan khusus layanan: Yes

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya menggunakan operasi `AND` logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan `OR` operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tanda yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, lihat Elemen kebijakan IAM: variabel dan tanda dalam Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Untuk melihat daftar kunci AWS Config kondisi, lihat Kunci kondisi untuk AWS Config dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang ditentukan oleh AWS Config.

Untuk melihat contoh kebijakan AWS Config berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk AWS Config

ACLs di AWS Config

Mendukung ACLs: Tidak

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan JSON.

ABAC dengan AWS Config

Mendukung ABAC (tanda dalam kebijakan): Ya

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak AWS sumber daya. Penandaan ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi ketika tanda milik prinsipal cocok dengan tanda yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna di situasi saat manajemen kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tanda, berikan informasi tentang tanda di elemen kondisi dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat Tentukan izin dengan otorisasi ABAC dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang menandai AWS Config sumber daya, lihatMenandai Sumber Daya Anda AWS Config.

Menggunakan kredensi sementara dengan AWS Config

Mendukung kredensial sementara: Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensil sementara. Untuk informasi tambahan, termasuk yang Layanan AWS bekerja dengan kredensi sementara, lihat Layanan AWS yang bekerja dengan IAM di Panduan Pengguna IAM.

Anda menggunakan kredensyal sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan tautan masuk tunggal (SSO) perusahaan Anda, proses tersebut secara otomatis membuat kredensil sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang peralihan peran, lihat Beralih dari pengguna ke peran IAM (konsol) dalam Panduan Pengguna IAM.

Anda dapat membuat kredenal sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensyal sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensyal sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM.

Teruskan sesi akses untuk AWS Config

Mendukung sesi akses maju (FAS): Ya

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.

Peran layanan untuk AWS Config

Mendukung peran layanan: Ya

Peran layanan adalah peran IAM yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.

> **Warning**
>
> Mengubah izin untuk peran layanan dapat merusak fungsionalitas AWS Config . Edit peran layanan hanya jika AWS Config memberikan panduan untuk melakukannya.

Peran terkait layanan untuk AWS Config

Mendukung peran terkait layanan: Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul

di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang membuat atau mengelola peran AWS Config terkait layanan, lihat. Menggunakan Peran Tertaut Layanan untuk AWS Config

Untuk detail tentang pembuatan atau manajemen peran terkait layanan, lihat Layanan AWS yang berfungsi dengan IAM. Cari layanan dalam tabel yang memiliki `Yes` di kolom Peran terkait layanan. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Contoh kebijakan berbasis identitas untuk AWS Config

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau mengubah sumber daya AWS Config . Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM dengan menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan IAM (konsol) di Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh AWS Config, termasuk format ARNs untuk setiap jenis sumber daya, lihat Kunci tindakan, sumber daya, dan kondisi untuk AWS Config dalam Referensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan
- Mendaftar untuk Akun AWS
- Buat pengguna dengan akses administratif
- Menggunakan konsol AWS Config
- Mengizinkan pengguna melihat izin mereka sendiri
- Akses hanya-baca ke AWS Config
- Akses penuh ke AWS Config
- Izin Tingkat Sumber Daya yang Didukung untuk Tindakan API Aturan AWS Config
- Izin Tingkat Sumber Daya yang Didukung untuk Agregasi Data Multi-Wilayah Multi-Akun

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus AWS Config sumber daya di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan dengan IAM Access Analyzer dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan.

Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Amankan akses API dengan MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan di IAM dalam Panduan Pengguna IAM.

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/pendaftaran.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan menerima panggilan telepon atau pesan teks dan memasukkan kode verifikasi pada keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS mengirimi Anda email konfirmasi setelah proses pendaftaran selesai. Kapan saja, Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan masuk https://aws.amazon.comke/ dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

Untuk bantuan masuk dengan menggunakan pengguna root, lihat Masuk sebagai pengguna root di AWS Sign-In Panduan Pengguna.

2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

   Untuk petunjuk, lihat Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root (konsol) Anda di Panduan Pengguna IAM.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

   Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .

2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

   Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email saat Anda membuat pengguna Pusat Identitas IAM.

  Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat Masuk ke portal AWS akses di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat Identitas IAM, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

   Untuk petunjuknya, lihat Membuat set izin di Panduan AWS IAM Identity Center Pengguna.

2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

   Untuk petunjuk, lihat Menambahkan grup di Panduan AWS IAM Identity Center Pengguna.

Menggunakan konsol AWS Config

Untuk mengakses AWS Config konsol, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang AWS Config sumber daya di Anda Akun AWS. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, izinkan akses hanya ke tindakan yang sesuai dengan operasi API yang coba mereka lakukan.

Untuk memastikan bahwa pengguna dan peran masih dapat menggunakan AWS Config konsol, lampirkan juga kebijakan AWS Config `AWSConfigUserAccess` AWS terkelola ke entitas. Untuk informasi selengkapnya, lihat Menambah izin untuk pengguna dalam Panduan Pengguna IAM.

Anda harus memberikan izin kepada pengguna untuk berinteraksi AWS Config. Untuk pengguna yang membutuhkan akses penuh AWS Config, gunakan kebijakan Akses penuh ke AWS Config terkelola.

Untuk memberikan akses dan menambahkan izin bagi pengguna, grup, atau peran Anda:

- Pengguna dan grup di AWS IAM Identity Center:

  Buat rangkaian izin. Ikuti instruksi di Buat rangkaian izin di Panduan Pengguna AWS IAM Identity Center .

- Pengguna yang dikelola di IAM melalui penyedia identitas:

  Buat peran untuk federasi identitas. Ikuti instruksi dalam Buat peran untuk penyedia identitas pihak ketiga (federasi) dalam Panduan Pengguna IAM.

- Pengguna IAM:
  - Buat peran yang dapat diambil pengguna Anda. Ikuti instruksi dalam Buat peran untuk pengguna IAM dalam Panduan Pengguna IAM.
  - (Tidak disarankan) Lampirkan kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti petunjuk dalam Menambahkan izin ke pengguna (konsol) dalam Panduan Pengguna IAM.

Mengizinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Akses hanya-baca ke AWS Config

Contoh berikut menunjukkan kebijakan AWS terkelola, `AWSConfigUserAccess` yang memberikan akses hanya-baca. AWS Config

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "config:Get*",
        "config:Describe*",
        "config:Deliver*",
        "config:List*",
        "config:Select*",
        "tag:GetResources",
        "tag:GetTagKeys",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

Dalam pernyataan kebijakan, `Effect` elemen menentukan apakah tindakan diizinkan atau ditolak. `Action`Elemen mencantumkan tindakan spesifik yang diizinkan dilakukan pengguna. `Resource`Elemen mencantumkan AWS sumber daya yang diizinkan pengguna untuk melakukan tindakan tersebut. Untuk kebijakan yang mengontrol akses ke AWS Config tindakan, `Resource` elemen selalu disetel ke`*`, wildcard yang berarti “semua sumber daya.”

Nilai-nilai dalam `Action` elemen sesuai dengan APIs yang didukung layanan. Tindakan didahului oleh `config:` untuk menunjukkan bahwa mereka merujuk AWS Config pada tindakan. Anda dapat menggunakan karakter `*` wildcard dalam `Action` elemen, seperti dalam contoh berikut:

- `"Action": ["config:*ConfigurationRecorder"]`

Ini memungkinkan semua AWS Config tindakan yang diakhiri dengan "ConfigurationRecorder" (`StartConfigurationRecorder`,`StopConfigurationRecorder`).

- `"Action": ["config:*"]`

  Ini memungkinkan semua AWS Config tindakan, tetapi bukan tindakan untuk AWS layanan lain.

- `"Action": ["*"]`

  Ini memungkinkan semua AWS tindakan. Izin ini cocok untuk pengguna yang bertindak sebagai AWS administrator untuk akun Anda.

Kebijakan hanya-baca tidak memberikan izin kepada pengguna untuk tindakan sepertiStartConfigurationRecorder,StopConfigurationRecorder, dan. `DeleteConfigurationRecorder` Pengguna dengan kebijakan ini tidak diizinkan untuk memulai perekam konfigurasi, menghentikan perekam konfigurasi, atau menghapus perekam konfigurasi. Untuk daftar AWS Config tindakan, lihat Referensi AWS Config API.

Akses penuh ke AWS Config

Contoh berikut menunjukkan kebijakan yang memberikan akses penuh ke AWS Config. Ini memberi pengguna izin untuk melakukan semua AWS Config tindakan. Ini juga memungkinkan pengguna mengelola file di bucket Amazon S3 dan mengelola topik Amazon SNS di akun yang dikaitkan dengan pengguna.

> **Important**
>
> Kebijakan ini memberikan izin yang luas. Sebelum memberikan akses penuh, pertimbangkan untuk memulai dengan set izin minimum dan memberikan izin tambahan seperlunya. Melakukannya adalah praktik yang lebih baik daripada memulai dengan izin yang terlalu lunak dan kemudian mencoba mengencangkannya nanti.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": [
                "sns:AddPermission",
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:GetTopicAttributes",
                "sns:ListPlatformApplications",
                "sns:ListTopics",
                "sns:SetTopicAttributes"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:GetBucketAcl",
                "s3:GetBucketLocation",
                "s3:GetBucketNotification",
                "s3:GetBucketPolicy",
                "s3:GetBucketRequestPayment",
                "s3:GetBucketVersioning",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:ListBucketVersions",
                "s3:PutBucketPolicy"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:ListRolePolicies",
                "iam:ListRoles",
                "iam:PutRolePolicy",
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
                "iam:CreatePolicyVersion",
                "iam:DeletePolicyVersion",
                "iam:CreateServiceLinkedRole"
```

```
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "config.amazonaws.com",
                        "ssm.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:LookupEvents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "config:*",
                "tag:Get*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeDocument",
                "ssm:GetDocument",
                "ssm:DescribeAutomationExecutions",
                "ssm:GetAutomationExecution",
                "ssm:ListDocuments",
                "ssm:StartAutomationExecution"
```

```
            ],
            "Resource": "*"
        }

    ]
}
```

Izin Tingkat Sumber Daya yang Didukung untuk Tindakan API Aturan AWS Config

Izin tingkat sumber daya mengacu pada kemampuan untuk menentukan sumber daya pengguna mana yang diizinkan untuk melakukan tindakan. AWS Config mendukung izin tingkat sumber daya untuk tindakan API aturan tertentu. AWS Config Ini berarti bahwa untuk tindakan AWS Config aturan tertentu, Anda dapat mengontrol kondisi di mana pengguna diizinkan untuk menggunakan tindakan tersebut. Kondisi ini dapat berupa tindakan yang harus dipenuhi, atau sumber daya tertentu yang diizinkan untuk digunakan pengguna.

Tabel berikut menjelaskan tindakan API AWS Config aturan yang saat ini mendukung izin tingkat sumber daya. Ini juga menjelaskan sumber daya yang didukung dan mereka ARNs untuk setiap tindakan. Saat menentukan ARN, Anda dapat menggunakan wildcard * di jalur Anda; misalnya, ketika Anda tidak dapat atau tidak ingin menentukan sumber daya yang tepat. IDs

> **Important**
>
> Jika tindakan API AWS Config aturan tidak tercantum dalam tabel ini, maka tindakan tersebut tidak mendukung izin tingkat sumber daya. Jika tindakan AWS Config aturan tidak mendukung izin tingkat sumber daya, Anda dapat memberikan izin kepada pengguna untuk menggunakan tindakan tersebut, tetapi Anda harus menentukan * untuk elemen sumber daya pernyataan kebijakan Anda.

Tindakan API	Sumber daya
DeleteConfigRule	Aturan Config arn:aws:config ::config-rule/config-rule- *region:accountID ID*
DeleteEvaluationResults	Aturan Config

Tindakan API	Sumber daya
	arn:aws:config ::config-rule/config-rule- *region:accountID ID*
DescribeCompliance ByConfigRule	Aturan Config arn:aws:config ::config-rule/config-rule- *region:accountID ID*
DescribeConfigRuleEvaluatio nStatus	Aturan Config arn:aws:config ::config-rule/config-rule- *region:accountID ID*
GetComplianceDetailsByConfi gRule	Aturan Config arn:aws:config ::config-rule/config-rule- *region:accountID ID*
PutConfigRule	Aturan Config arn:aws:config ::config-rule/config-rule- *region:accountID ID*
StartConfigRulesEvaluation	Aturan Config arn:aws:config ::config-rule/config-rule- *region:accountID ID*
PutRemediationConfigurations	Konfigurasi Remediasi arn:aws:config ::remediation-configuration/ *region:ac countId config rule name/remediation configura tion id*
DescribeRemediationConfigur ations	Konfigurasi Remediasi arn:aws:config ::remediation-configuration/ *region:ac countId config rule name/remediation configura tion id*

Tindakan API	Sumber daya
DeleteRemediationConfiguration	Konfigurasi Remediasi arn:aws:config ::remediation-configuration/ *region:accountId config rule name/remediation configuration id*
PutRemediationExceptions	Konfigurasi Remediasi arn:aws:config ::remediation-configuration/ *region:accountId config rule name/remediation configuration id*
DescribeRemediationExceptions	Konfigurasi Remediasi arn:aws:config ::remediation-configuration/ *region:accountId config rule name/remediation configuration id*
DeleteRemediationExceptions	Konfigurasi Remediasi arn:aws:config ::remediation-configuration/ *region:accountId config rule name/remediation configuration id*

Misalnya, Anda ingin mengizinkan akses baca dan menolak akses tulis ke aturan tertentu untuk pengguna tertentu.

Dalam kebijakan pertama, Anda mengizinkan tindakan membaca AWS Config aturan seperti `DescribeConfigRuleEvaluationStatus` pada aturan yang ditentukan.

JSON

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "VisualEditor0",
```

```
                "Effect": "Allow",
                "Action": [
                    "config:StartConfigRulesEvaluation",
                    "config:DescribeComplianceByConfigRule",
                    "config:DescribeConfigRuleEvaluationStatus",
                    "config:GetComplianceDetailsByConfigRule"
                ],
                "Resource": [
                    "arn:aws:config:region:accountID:config-rule/config-rule-ID",
                    "arn:aws:config:region:accountID:config-rule/config-rule-ID"
                ]
            }
        ]
    }
```

Dalam kebijakan kedua, Anda menolak AWS Config aturan menulis tindakan pada aturan tertentu.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": [
                "config:PutConfigRule",
                "config:DeleteConfigRule",
                "config:DeleteEvaluationResults"
               ],
            "Resource": "arn:aws:config:region:accountID:config-rule/config-
rule-ID"
           }
      ]
   }
```

Dengan izin tingkat sumber daya, Anda dapat mengizinkan akses baca dan menolak akses tulis untuk melakukan tindakan tertentu pada tindakan API aturan. AWS Config

Izin Tingkat Sumber Daya yang Didukung untuk Agregasi Data Multi-Wilayah Multi-Akun

Anda dapat menggunakan izin tingkat sumber daya untuk mengontrol kemampuan pengguna untuk melakukan tindakan tertentu pada agregasi data multi-wilayah multi-akun. Izin tingkat sumber daya AWS Config `Aggregator` APIs dukungan berikut:

- BatchGetAggregateResourceConfig
- DeleteConfigurationAggregator
- DescribeAggregateComplianceByConfigRules
- DescribeAggregateComplianceByConformancePacks
- DescribeConfigurationAggregatorSourcesStatus
- GetAggregateComplianceDetailsByConfigRule
- GetAggregateConfigRuleComplianceSummary
- GetAggregateConformancePackComplianceSummary
- GetAggregateDiscoveredResourceCounts
- GetAggregateResourceConfig
- ListAggregateDiscoveredResources
- PutConfigurationAggregator
- SelectAggregateResourceConfig

Misalnya, Anda dapat membatasi akses ke data sumber daya dari pengguna tertentu dengan membuat dua agregator `AccessibleAggregator` `InAccessibleAggregator` dan melampirkan kebijakan IAM yang memungkinkan akses ke tetapi menolak akses ke`AccessibleAggregator`. `InAccessibleAggregator`

Kebijakan IAM untuk AccessibleAggregator

Dalam kebijakan ini, Anda mengizinkan akses ke tindakan agregator yang didukung untuk Nama Sumber Daya AWS Config Amazon (ARN) yang Anda tentukan. Dalam contoh ini, AWS Config ARN adalah. `arn:aws:config:ap-northeast-1:`*`AccountID`*`:config-aggregator/config-aggregator-mocpsqhs`

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigAllow",
            "Effect": "Allow",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-
aggregator/config-aggregator-mocpsqhs"
        }
    ]
}
```

Kebijakan IAM untuk InAccessibleAggregator

Dalam kebijakan ini, Anda menolak akses ke tindakan agregator yang didukung untuk AWS Config ARN yang Anda tentukan. Dalam contoh ini, AWS Config ARN adalah. `arn:aws:config:ap-northeast-1:`*`AccountID`*`:config-aggregator/config-aggregator-pokxzldx`

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "ConfigDeny",
            "Effect": "Deny",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-
aggregator/config-aggregator-pokxzldx"
        }
    ]
}
```

Jika pengguna grup pengembang mencoba melakukan salah satu tindakan ini pada AWS Config ARN yang Anda tentukan, pengguna tersebut akan mendapatkan pengecualian akses yang ditolak.

Memeriksa Izin Akses Pengguna

Untuk menampilkan agregator yang telah Anda buat, jalankan perintah berikut: AWS CLI

```
aws configservice describe-configuration-aggregators
```

Ketika perintah telah berhasil diselesaikan, Anda akan dapat melihat rincian untuk semua agregator yang terkait dengan akun Anda. Dalam contoh ini, mereka adalah `AccessibleAggregator` dan`InAccessibleAggregator`:

```
{
    "ConfigurationAggregators": [
        {
            "ConfigurationAggregatorArn": "arn:aws:config:ap-
northeast-1:AccountID:config-aggregator/config-aggregator-mocpsqhs",
```

```
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "AccessibleAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        },
        {
            "ConfigurationAggregatorArn": "arn:aws:config:ap-
northeast-1:AccountID:config-aggregator/config-aggregator-pokxzldx",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "InAccessibleAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        }
    ]
}
```

> **Note**
>
> Untuk `account-aggregation-sources` masukkan daftar AWS akun IDs yang dipisahkan koma yang ingin Anda agregat datanya. Bungkus akun IDs dalam tanda kurung siku, dan pastikan untuk menghindari tanda kutip (misalnya,`"[{\"AccountIds\": [\"AccountID1\",\"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"`).

Lampirkan kebijakan IAM berikut untuk menolak akses`InAccessibleAggregator`, atau agregator yang ingin Anda tolak aksesnya.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigDeny",
            "Effect": "Deny",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-
aggregator/config-aggregator-pokxzldx"
        }
    ]
}
```

Selanjutnya, Anda dapat mengonfirmasi bahwa kebijakan IAM berfungsi untuk membatasi akses ke aturan untuk agregator tertentu:

```
aws configservice get-aggregate-compliance-details-by-config-rule --configuration-
aggregator-name InAccessibleAggregator --config-rule-name rule name --account-
id AccountID --aws-region AwsRegion
```

Perintah harus mengembalikan pengecualian akses yang ditolak:

```
An error occurred (AccessDeniedException) when calling the
 GetAggregateComplianceDetailsByConfigRule operation: User:
 arn:aws:iam::AccountID:user/ is not
authorized to perform: config:GetAggregateComplianceDetailsByConfigRule on resource:
 arn:aws:config:AwsRegion-1:AccountID:config-aggregator/config-aggregator-pokxzldx
```

AWS kebijakan terkelola untuk AWS Config

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS Kebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pembaruan akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat Kebijakan terkelola AWS dalam Panduan Pengguna IAM.

AWS kebijakan terkelola: AWSConfigServiceRolePolicy

AWS Config menggunakan peran terkait layanan yang diberi nama AWSServiceRoleForConfiguntuk memanggil AWS layanan lain atas nama Anda. Ketika Anda menggunakan AWS Management Console to set up AWS Config, SLR ini secara otomatis dibuat oleh AWS Config jika Anda memilih opsi untuk menggunakan AWS Config SLR alih-alih peran layanan Anda sendiri AWS Identity and Access Management (IAM).

AWSServiceRoleForConfigSLR berisi kebijakan `AWSConfigServiceRolePolicy` terkelola. Kebijakan terkelola ini berisi izin hanya-baca dan hanya-tulis untuk AWS Config sumber daya dan izin hanya-baca untuk sumber daya di layanan lain yang mendukung. AWS Config Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config dan Menggunakan Peran Tertaut Layanan untuk AWS Config.

Lihat kebijakan: AWSConfigServiceRolePolicy.

> Direkomendasikan: Gunakan peran terkait Layanan
>
> Disarankan agar Anda menggunakan peran terkait layanan kecuali Anda memiliki kasus penggunaan tertentu. Peran terkait layanan menambahkan semua izin yang diperlukan untuk menjalankan seperti yang AWS Config diharapkan. Beberapa fitur seperti perekam konfigurasi terkait layanan mengharuskan Anda untuk menggunakan peran terkait layanan.

AWS kebijakan terkelola: AWS_ConfigRole

Untuk merekam konfigurasi AWS sumber daya Anda, AWS Config memerlukan izin IAM untuk mendapatkan detail konfigurasi tentang sumber daya Anda. Jika Anda ingin membuat peran IAM AWS Config, Anda dapat menggunakan kebijakan terkelola `AWS_ConfigRole` dan melampirkannya ke peran IAM Anda.

Kebijakan IAM ini diperbarui setiap kali AWS Config menambahkan dukungan untuk jenis AWS sumber daya. Ini berarti bahwa AWS Config akan terus memiliki izin yang diperlukan untuk merekam data konfigurasi tipe sumber daya yang didukung selama peran AWS_ConFigRole memiliki kebijakan terkelola ini dilampirkan. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config dan Izin untuk Peran IAM Ditugaskan AWS Config.

Lihat kebijakan: AWS_COnFigRole.

AWS kebijakan terkelola: AWSConfigUserAccess

Kebijakan IAM ini menyediakan akses untuk digunakan AWS Config, termasuk mencari berdasarkan tag pada sumber daya dan membaca semua tag. Ini tidak memberikan izin untuk mengkonfigurasi AWS Config, yang membutuhkan hak administratif.

Lihat kebijakan: AWSConfigUserAccess.

AWS kebijakan terkelola: ConfigConformsServiceRolePolicy

Untuk menyebarkan dan mengelola paket kesesuaian, AWS Config memerlukan izin IAM dan izin tertentu dari layanan lain. AWS Ini memungkinkan Anda untuk menyebarkan dan mengelola paket kesesuaian dengan fungsionalitas penuh dan diperbarui setiap kali AWS Config menambahkan fungsionalitas baru untuk paket kesesuaian. Untuk informasi selengkapnya tentang paket kesesuaian, lihat Paket kesesuaian.

Lihat kebijakan: ConfigConformsServiceRolePolicy.

AWS kebijakan terkelola: AWSConfigRulesExecutionRole

Untuk menerapkan Aturan Lambda AWS Kustom AWS Config , memerlukan izin IAM dan izin tertentu dari layanan lain. AWS Ini memungkinkan AWS Lambda fungsi untuk mengakses AWS Config API dan snapshot konfigurasi yang AWS Config dikirimkan secara berkala ke Amazon S3. Akses ini diperlukan oleh fungsi yang mengevaluasi perubahan konfigurasi untuk aturan Lambda AWS Kustom dan diperbarui setiap kali AWS Config menambahkan fungsionalitas baru. Untuk informasi selengkapnya tentang Aturan Lambda AWS Kustom, lihat Membuat Aturan AWS Config Lambda Kustom. Untuk informasi selengkapnya tentang snapshot konfigurasi, lihat Concepts | Configuration Snapshot. Untuk informasi selengkapnya tentang pengiriman snapshot konfigurasi, lihat Mengelola Saluran Pengiriman.

Lihat kebijakan: AWSConfigRulesExecutionRole.

AWS kebijakan terkelola: AWSConfigMultiAccountSetupPolicy

Untuk menyebarkan, memperbarui, dan menghapus AWS Config aturan dan paket kesesuaian secara terpusat di seluruh akun anggota dalam organisasi AWS Organizations, AWS Config memerlukan izin IAM dan izin tertentu dari layanan lain. AWS Kebijakan terkelola ini diperbarui setiap kali AWS Config menambahkan fungsionalitas baru untuk penyiapan multi-akun. Untuk informasi selengkapnya, lihat Mengelola AWS Config Aturan di Semua Akun di Organisasi Anda dan Mengelola Paket Kesesuaian di Semua Akun di Organisasi Anda.

Lihat kebijakan: AWSConfigMultiAccountSetupPolicy.

AWS kebijakan terkelola: AWSConfigRoleForOrganizations

AWS Config Untuk memungkinkan panggilan hanya-baca AWS Organizations APIs, AWS Config memerlukan izin IAM dan izin tertentu dari layanan lain. AWS Kebijakan terkelola ini diperbarui setiap kali AWS Config menambahkan fungsionalitas baru untuk penyiapan multi-akun. Untuk informasi selengkapnya, lihat Mengelola AWS Config Aturan di Semua Akun di Organisasi Anda dan Mengelola Paket Kesesuaian di Semua Akun di Organisasi Anda.

Lihat kebijakan: AWSConfigRoleForOrganizations.

Kebijakan terkelola AWS : AWSConfigRemediationServiceRolePolicy

Untuk AWS Config memperbolehkan memulihkan `NON_COMPLIANT` sumber daya atas nama Anda, AWS Config memerlukan izin IAM dan izin tertentu dari layanan lain. AWS Kebijakan terkelola

ini diperbarui setiap kali AWS Config menambahkan fungsionalitas baru untuk remediasi. Untuk informasi selengkapnya tentang remediasi, lihat Remediating Noncompliant Resources with Rules. AWS Config Untuk informasi lebih lanjut tentang kondisi yang memulai kemungkinan hasil AWS Config evaluasi, lihat Konsep | AWS Config Aturan.

Lihat kebijakan: AWSConfigRemediationServiceRolePolicy.

AWS Config pembaruan kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola AWS Config sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman Riwayat AWS Config dokumen.

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan “backup-gateway: GetHypervisor “, “backup-gateway: “,": ListHypervisors “,"bcm-data-exports: GetExport “,"bcm-data-exports: ListExports “, “batuan dasarbcm-data-exports: ListTagsForResource “, “batuan dasar: GetAgent “, “batuan dasar: GetAgentActionGroup “, “batuan dasar: GetAgentKnowledgeBase “, “batuan dasar: GetDataSource “, “batuan dasar: GetFlowAlias “, “batuan dasar: GetFlowVersion “, “batuan dasar: ListAgentActionGroups “, “batuan dasar: ListAgentKnowledgeBases “, “cloudformation: ListDataSources “, “cloudformation: “, ListFlowAliases	Kebijakan ini sekarang mendukung izin tambahan untuk AWS Backup gateway, AWS Manajemen Penagihan dan Biaya, Amazon Bedrock,, AWS CloudFormation Amazon CloudFront,, Resolusi Entitas AWS, AWS IoT Core Device Advisor, AWS Lambda, AWS Network Manager, AWS Private Certificate Authority , Amazon Redshift, Tabel Amazon S3,. Pengaturan Cepat AWS Systems Manager	Juni 18, 2025

Perubahan	Deskripsi	Tanggal
“cloudformation: “, ListFlowVersions “cloudformation: “,” BatchDescribeTypeConfigurations DescribeStackInstance DescribeStackSet ListStackInstances cloudformation: ListStackSets “, “cloudfront: “, “cloudfront: GetPublicKey “, “cloudfront: GetRealtimeLogConfig “, “cloudfront: “, “entityresolution: ListPublicKeys “, “entityresolution: ListRealtimeLogConfigs “, “entityresolution: “, “entityresolution: GetIdMappingWorkflow “, “entityresolution: GetSchemaMapping “, “iotdeviceadvisor: ListIdMappingWorkflows “, “iotdeviceadvisor: ListSchemaMappings “, “lambda: “, “lambda: ListTagsForResource “, “mediapackagev2: “, “mediapackagev2: GetSuiteDefinition “, “networkmanager: “, “networkmanager: ListSuiteDefinitions “,": “,” GetEventSourceMapping ListEventSourceMappings GetChannel ListChannels GetTransitGatewayPeering ListPeerings pca-connector-ad GetDirectoryRegistration pca-connector-ad: ListDirectoryRegistrations “,"pca-connector-a		

Perubahan	Deskripsi	Tanggal
d: ListTagsForResource “, “rds:Deskripsikan DBShard Grup”, “rds: “, “pergeseran merah: DescribeIntegrations “, “s3tables: DescribeIntegratio ns “, “s3tables: “, “s3tables: GetTableBucket “, “s3tables: GetTableBucketEncryption “, “ssm-quicksetup: GetTableB ucketMaintenanceConfigurati on “, “ssm-quicksetup:” ListTableBuckets GetConfig urationManager ListConfi gurationManagers		

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan “backup-gateway: GetHypervisor “, “backup-gateway: “,": ListHyper visors “,"bcm-data-export s: GetExport “,"bcm-data-exports: ListExports “, “batuan dasarbcm-data-exports: ListTagsForResource “, “batuan dasar: GetAgent “, “batuan dasar: GetAgentA ctionGroup “, “batuan dasar: GetAgentKnowledgeBase “, “batuan dasar: GetDataSo urce “, “batuan dasar: GetFlowAlias “, “batuan dasar: GetFlowVersion “, “batuan dasar: ListAgent ActionGroups “, “batuan dasar: ListAgentKnowledge Bases “, “cloudformation: ListDataSources “, “cloudfor mation: “, ListFlowAliases “cloudformation: “, ListFlowV ersions “cloudformation: “,” BatchDescribeTypeC onfigurations DescribeS tackInstance DescribeS tackSet ListStackInstances cloudformation: ListStack Sets “, “cloudfront: “, “cloudfro nt: GetPublicKey “, “cloudfro nt: GetRealtimeLogConfig “, “cloudfront: “, ListPubli	Kebijakan ini sekarang mendukung izin tambahan untuk AWS Backup gateway, AWS Manajemen Penagihan dan Biaya, Amazon Bedrock,, AWS CloudFormation Amazon CloudFront,, Resolusi Entitas AWS, AWS IoT Core Device Advisor, AWS Lambda, AWS Network Manager, AWS Private Certificate Authority , Amazon Redshift, Tabel Amazon S3,. Pengaturan Cepat AWS Systems Manager	Juni 18, 2025

Perubahan	Deskripsi	Tanggal
cKeys “entityresolution: “, “entityresolution: ListRealt imeLogConfigs “, “entityre solution: GetIdMappingWorkfl ow “, “entityresolution: “, “entityresolution: GetSchema Mapping “, “iotdeviceadvisor: ListIdMappingWorkflows “, “iotdeviceadvisor: ListSchem aMappings “, “lambda: ListTagsForResource “, “lambda: “, “networkm anager: GetSuiteDefinition “, “networkmanager: “,": “,ListSui teDefinitions": “,": “, “rds: GetEventSourceMapping ListEventSourceMappings GetTransitGatewayPeering ListPeerings pca-connector-ad GetDirectoryRegistration pca-connector-ad ListDirec toryRegistrations pca-conne ctor-ad ListTagsForResourc e Jelaskan DBShard Grup”, “rds: “, DescribeIntegratio ns “pergeseran merah: “, “s3tables: Describel ntegrations “, “s3tables: GetTableBucket “, “s3tables : “, GetTableBucketEncr yption “s3tables: “, “ssm-quic ksetup: GetTableBucketMain tenanceConfiguration “, “ssm-quicksetup:ListTableBuckets”		

Perubahan	Deskripsi	Tanggal
GetConfigurationManager ListConfigurationManagers		
AWS_ConfigRole— Tambahkan "bedrock: GetGuardrail", "bedrock: GetInferenceProfile", "bedr ock:GetKnowledgeBase", "bedrock:ListGuardrails", " bedrock:ListInferenceProfiles", "bedrock:ListKnowledgeBases ", "bedrock:ListTagsForReso urce"	Kebijakan ini sekarang mendukung izin tambahan untuk Amazon Bedrock.	27 Mei 2025
AWSConfigServiceRo lePolicy— Tambahkan "bedrock:GetGuardrail", "bedrock:GetInferenceProfile", "bedrock:GetKnowledgeBase", "bedrock:ListGuardrails", " bedrock:ListInferenceProfiles", "bedrock:ListKnowledgeBases ", "bedrock:ListTagsForReso urce"	Kebijakan ini sekarang mendukung izin tambahan untuk Amazon Bedrock.	27 Mei 2025

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan "b2bi:GetPartnership", "b2bi:GetProfile", "b2bi:ListPartnerships", "b2bi:ListProfiles", "bedrock:ListAgents", "cleanrooms:GetConfiguredTable", "cleanrooms:GetConfiguredTableAnalysisRule", "cleanrooms:GetMembership", "cleanrooms:GetPrivacyBudgetTemplate", "cleanrooms:ListConfiguredTables", "cleanrooms:ListMemberships", "cleanrooms:ListPrivacyBudgetTemplates", "codeconnections:GetConnection", "codeconnections:ListConnections", "codeconnections:ListTagsForResource", "directconnect:DescribeConnections", "dms:DescribeReplicationConfigs", "logs:DescribeAccountPolicies", "logs:DescribeResourcePolicies", "macie2:ListAutomatedDiscoveryAccounts", "managedblockchain:GetAccessor", "managedblockchain:ListAccessors", "qbusiness:GetApplication", "qbusiness:ListApplications", "qbusiness:ListTagsForResource", "route53profiles:GetProfile", "route53profiles:GetProfile	Kebijakan ini sekarang mendukung izin tambahan untuk AWS B2B Pertukaran Data, Amazon Bedrock,, ,, AWS Database Migration Service (AWS DMS) AWS Clean Rooms AWS CodeConnections, Amazon CloudWatch Log AWS Direct Connect, Amazon Macie, Amazon Managed Blockchain, Amazon Q Business, Route 53 Profiles, Amazon Simple Storage Service (Amazon S3), SageMaker Amazon AWS Security Hub AI,, dan, Kontak, dan. Manajer Insiden AWS Systems Manager Manajer Insiden AWS Systems Manager AWS Systems Manager	April 08, 2025

Perubahan	Deskripsi	Tanggal
Association", "route53profiles:ListProfileAssociations", "route53profiles:ListProfiles", "route53profiles:ListTagsForResource", "s3:GetAccessGrantsInstance", "s3:GetAccessGrantsLocation", "s3:ListAccessGrantsInstances", "s3:ListAccessGrantsLocations", "sagemaker:DescribeCluster", "sagemaker:DescribeMlflowTrackingServer", "sagemaker:DescribeStudioLifecycleConfig", "sagemaker:ListClusters", "sagemaker:ListMlflowTrackingServers", "sagemaker:ListStudioLifecycleConfigs", "securityhub:DescribeStandardsControls", "securityhub:GetEnabledStandards", "ssm-contacts:GetContact", "ssm-contacts:GetContactChannel", "ssm-contacts:ListContactChannels", "ssm-contacts:ListContacts", "ssm-incidents:GetResponsePlan", "ssm-incidents:ListResponsePlans", "ssm-incidents:ListTagsForResource", "ssm:DescribeInstanceInformation"		

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan "b2bi:GetPartnership", "b2bi:GetProfile", "b2bi:ListPartnerships", "b2bi:ListProfiles", "bedrock:ListAgents", "cleanrooms:GetConfiguredTable", "cleanrooms:GetConfiguredTableAnalysisRule", "cleanrooms:GetMembership", "cleanrooms:GetPrivacyBudgetTemplate", "cleanrooms:ListConfiguredTables", "cleanrooms:ListMemberships", "cleanrooms:ListPrivacyBudgetTemplates", "codeconnections:GetConnection", "codeconnections:ListConnections", "codeconnections:ListTagsForResource", "directconnect:DescribeConnections", "dms:DescribeReplicationConfigs", "logs:DescribeAccountPolicies", "logs:DescribeResourcePolicies", "macie2:ListAutomatedDiscoveryAccounts", "managedblockchain:GetAccessor", "managedblockchain:ListAccessors", "qbusiness:GetApplication", "qbusiness:ListApplications", "qbusiness:ListTagsForResource", "route53profiles:GetProfile", "route53profiles:GetProfile	Kebijakan ini sekarang mendukung izin tambahan untuk AWS B2B Pertukaran Data, Amazon Bedrock,, ,, AWS Database Migration Service (AWS DMS) AWS Clean Rooms AWS CodeConnections, Amazon CloudWatch Log AWS Direct Connect, Amazon Macie, Amazon Managed Blockchain, Amazon Q Business, Route 53 Profiles, Amazon Simple Storage Service (Amazon S3), SageMaker Amazon AWS Security Hub AI,, dan, Kontak, dan. Manajer Insiden AWS Systems Manager Manajer Insiden AWS Systems Manager AWS Systems Manager Kebijakan ini juga sekarang mendukung izin untuk mengakses semua nama domain Amazon API Gateway dengan menyertakan pola sumber daya "`arn:aws:apigateway:::/domainnames/`".	April 08, 2025

Perubahan	Deskripsi	Tanggal
Association", "route53profiles:ListProfileAssociations", "route53profiles:ListProfiles", "route53profiles:ListTagsForResource", "s3:GetAccessGrantsInstance", "s3:GetAccessGrantsLocation", "s3:ListAccessGrantsInstances", "s3:ListAccessGrantsLocations", "sagemaker:DescribeCluster", "sagemaker:DescribeMlflowTrackingServer", "sagemaker:DescribeStudioLifecycleConfig", "sagemaker:ListClusters", "sagemaker:ListMlflowTrackingServers", "sagemaker:ListStudioLifecycleConfigs", "securityhub:DescribeStandardsControls", "securityhub:GetEnabledStandards", "ssm-contacts:GetContact", "ssm-contacts:GetContactChannel", "ssm-contacts:ListContactChannels", "ssm-contacts:ListContacts", "ssm-incidents:GetResponsePlan", "ssm-incidents:ListResponsePlans", "ssm-incidents:ListTagsForResource", "ssm:DescribeInstanceInformation"		

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan "ec2:GetAllowedImagesSettings"	Kebijakan ini sekarang mendukung izin tambahan untuk Amazon Elastic Compute Cloud (Amazon EC2).	Maret 4, 2025
AWSConfigServiceRolePolicy— Tambahkan "ec2:GetAllowedImagesSettings"	Kebijakan ini sekarang mendukung izin tambahan untuk Amazon Elastic Compute Cloud (Amazon EC2).	Maret 4, 2025

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan "cleanrooms-ml:GetTrainingDataset", "cleanrooms-ml:ListTrainingDatasets", "comprehend:DescribeFlywheel", "comprehend:ListFlywheels", "comprehend:ListTagsForResource", "ec2:GetSnapshotBlockPublicAccessState", "omics:GetAnnotationStore", "omics:GetRunGroup", "omics:GetSequenceStore", "omics:GetVariantStore", "omics:ListAnnotationStores", "omics:ListRunGroups", "omics:ListSequenceStores", "omics:ListTagsForResource", "omics:ListVariantStores", "s3express:GetEncryptionConfiguration", "s3express:GetLifecycleConfiguration", "ses:GetDedicatedIpPool", "ses:GetDedicatedIps", and "ses:ListDedicatedIpPools"	Kebijakan ini sekarang mendukung izin tambahan untuk AWS Clean Rooms, Amazon Comprehend, Amazon Elastic Compute Cloud (Amazon),, EC2 Amazon Simple Storage Service (Amazon S3) AWS HealthOmics, dan Amazon Simple Email Service (Amazon SES).	Januari 16, 2025

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan "cleanrooms-ml:GetTrainingDataset", "cleanrooms-ml:ListTrainingDatasets", "comprehend:DescribeFlywheel", "comprehend:ListFlywheels", "comprehend:ListTagsForResource", "ec2:GetSnapshotBlockPublicAccessState", "omics:GetAnnotationStore", "omics:GetRunGroup", "omics:GetSequenceStore", "omics:GetVariantStore", "omics:ListAnnotationStores", "omics:ListRunGroups", "omics:ListSequenceStores", "omics:ListTagsForResource", "omics:ListVariantStores", "s3express:GetEncryptionConfiguration", "s3express:GetLifecycleConfiguration", "ses:GetDedicatedIpPool", "ses:GetDedicatedIps", and "ses:ListDedicatedIpPools"	Kebijakan ini sekarang mendukung izin tambahan untuk AWS Clean Rooms, Amazon Comprehend, Amazon Elastic Compute Cloud (Amazon),, EC2 Amazon Simple Storage Service (Amazon S3) AWS HealthOmics, dan Amazon Simple Email Service (Amazon SES).	Januari 16, 2025
AWSConfigServiceRolePolicy— Tambahkan "organizations:ListAWSServiceAccessForOrganization"	Kebijakan ini sekarang mendukung izin tambahan untuk AWS Organizations.	Desember 18, 2024

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan "app-integrations: GetApplication", "app-integ rations:ListApplications", "app-integrations:ListTagsF orResource", "appconfig:Get Extension", "appconfig:ListExt ensions", "cloudtrail:GetIn sightSelectors", "connect: DescribeQueue", "connect:De scribeRoutingProfile", "con nect:DescribeSecurityProfil e", "connect:ListQueueQuick Connects", "connect: ListQueues", "connect:ListR outingProfileQueues", "conn ect:ListRoutingProfiles", " connect:ListSecurityProfile Applications", "connect:Lis tSecurityProfilePermissions ", "connect:ListSecurityPro files", "datazone:GetDomai n", "datazone:ListDomains", "devops-guru:ListNotificati onChannels", "glue:GetRegis try", "glue:ListRegistries", "ide ntitystore:DescribeGroup", "identitystore:DescribeGrou pMembership" "identitystore :ListGroupMemberships", "identitystore:ListGroups", "iot:DescribeThingGroup", "iot:DescribeThingType", "iot:ListThingGroups", "iot	Kebijakan ini sekarang mendukung izin tambahan untuk AWS AppConfig,, Amazon Connect, Amazon AWS CloudTrail, Amazon DevOps Guru,, Toko Identitas DataZone,,,, AWS Glue, Layanan Video Interakti f Amazon (Amazon IVS) AWS IoT AWS IoT FleetWise AWS IoT Wireless, Amazon CloudWatch Logs, Amazon Observability Access Manager,, Amazon AW S Payment Cryptography Relational Database Service (CloudWatch Amazon RDS), Amazon Rekognition, Amazon Simple Storage Service (Amazon Storage Service) 3) Simple Storage S3), Amazon Scheduler,, dan Amazon VPC Lattice. EventBridge AWS Systems Manager	November 7, 2024

Perubahan	Deskripsi	Tanggal
:ListThingTypes", "iotfleet wise:GetDecoderManifest", " iotfleetwise:GetFleet", "iotfleet wise:GetModelManifest", "io tfleetwise:GetSignalCatalog ", "iotfleetwise:GetVehicle", "iotfleetwise:ListDecoderMa nifestNetworkInterfaces", " iotfleetwise:ListDecoderMan ifests", "iotfleetwise:List DecoderManifestSignals", "iotfleetwise:ListFleets", "i otfleetwise:ListModelManife stNodes", "iotfleetwise:Lis tModelManifests", "iotfleet wise:ListSignalCatalogNodes ", "iotfleetwise:ListSignal Catalogs", "iotfleetwise:Li stTagsForResource", "iotfleet wise:ListVehicles", "iotwir eless:GetDestination", "iotwirel ess:GetDeviceProfile", "iot wireless:GetWirelessGateway ", "iotwireless:ListDestina tions", "iotwireless:ListDe viceProfiles", "iotwireless :ListWirelessGateways", "iv schat:GetLoggingConfigurati on", "ivschat:GetRoom" "ivschat:ListLoggingConfigu rations", "ivschat:ListRooms ", "ivschat:ListTagsForReso urce", "logs:GetLogAnomal yDetector", "logs:ListLogAn omalyDetectors", "oam:GetS		

Perubahan	Deskripsi	Tanggal
ink" "oam:GetSinkPolicy", "oam:ListSinks", "payment-cryptography:GetAlias", "payment-cryptography:GetKey", "payment-cryptography:ListAliases", "payment-cryptography:ListKeys", "payment-cryptography:ListTagsForResource", "rds:DescribeDBProxyTargetGroups", "rds:DescribeDBProxyTargets", "rekognition:DescribeProjects", "s3:GetStorageLensGroup", "s3:ListStorageLensGroups", "s3:ListTagsForResource", "scheduler:GetScheduleGroup", "scheduler:ListScheduleGroups", "scheduler:ListTagsForResource", "ssm:GetServiceSetting", "vpc-lattice:GetAccessLogSubscription", "vpc-lattice:GetService", "vpc-lattice:GetServiceNetwork", "vpc-lattice:GetTargetGroup", "vpc-lattice:ListAccessLogSubscriptions", "vpc-lattice:ListServiceNetworks", "vpc-lattice:ListServices", "vpc-lattice:ListTagsForResource", "vpc-lattice:ListTargetGroups", and "vpc-lattice:ListTargets"		

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan "app-integrations:GetApplication", "app-integrations:ListApplications", "app-integrations:ListTagsForResource", "appconfig:GetExtension", "appconfig:ListExtensions", "cloudtrail:GetInsightSelectors", "connect:DescribeQueue", "connect:DescribeRoutingProfile", "connect:DescribeSecurityProfile", "connect:ListQueueQuickConnects", "connect:ListQueues", "connect:ListRoutingProfileQueues", "connect:ListRoutingProfiles", "connect:ListSecurityProfileApplications", "connect:ListSecurityProfilePermissions", "connect:ListSecurityProfiles", "datazone:GetDomain", "datazone:ListDomains", "devops-guru:ListNotificationChannels", "glue:GetRegistry", "glue:ListRegistries", "identitystore:DescribeGroup", "identitystore:DescribeGroupMembership" "identitystore:ListGroupMemberships", "identitystore:ListGroups", "iot:DescribeThingGroup", "iot:DescribeThingType",	Kebijakan ini sekarang mendukung izin tambahan untuk AWS AppConfig,, Amazon Connect, Amazon AWS CloudTrail, Amazon DevOps Guru,, Toko Identitas DataZone,,,, AWS Glue, Layanan Video Interaktif Amazon (Amazon IVS) AWS IoT AWS IoT FleetWise AWS IoT Wireless, Amazon CloudWatch Logs, Amazon Observability Access Manager,, Amazon AWS Payment Cryptography Relational Database Service (CloudWatch Amazon RDS), Amazon Rekognition, Amazon Simple Storage Service (Amazon Storage Service) 3) Simple Storage S3), Amazon Scheduler,, dan Amazon VPC Lattice. EventBridge AWS Systems Manager	November 7, 2024

Perubahan	Deskripsi	Tanggal
"iot:ListThingGroups", "iot :ListThingTypes", "iotfleet wise:GetDecoderManifest", " iotfleetwise:GetFleet", "iotfleet wise:GetModelManifest", "io tfleetwise:GetSignalCatalog ", "iotfleetwise:GetVehicle", "iotfleetwise:ListDecoderMa nifestNetworkInterfaces", " iotfleetwise:ListDecoderMan ifests", "iotfleetwise:List DecoderManifestSignals", "iotfleetwise:ListFleets", "i otfleetwise:ListModelManife stNodes", "iotfleetwise:Lis tModelManifests", "iotfleet wise:ListSignalCatalogNodes ", "iotfleetwise:ListSignal Catalogs", "iotfleetwise:Li stTagsForResource", "iotfleet wise:ListVehicles", "iotwir eless:GetDestination", "iotwirel ess:GetDeviceProfile", "iot wireless:GetWirelessGateway ", "iotwireless:ListDestina tions", "iotwireless:ListDe viceProfiles", "iotwireless :ListWirelessGateways", "iv schat:GetLoggingConfigurati on", "ivschat:GetRoom" "ivschat:ListLoggingConfigu rations", "ivschat:ListRooms ", "ivschat:ListTagsForReso urce", "logs:GetLogAnomal yDetector", "logs:ListLogAn		

Perubahan	Deskripsi	Tanggal
omalyDetectors", "oam:GetSink" "oam:GetSinkPolicy", "oam:ListSinks", "payment-cryptography:GetAlias", "payment-cryptography:GetKey", "payment-cryptography:ListAliases", "payment-cryptography:ListKeys", "payment-cryptography:ListTagsForResource", "rds:DescribeDBProxyTargetGroups", "rds:DescribeDBProxyTargets", "rekognition:DescribeProjects", "s3:GetStorageLensGroup", "s3:ListStorageLensGroups", "s3:ListTagsForResource", "scheduler:GetScheduleGroup", "scheduler:ListScheduleGroups", "scheduler:ListTagsForResource", "ssm:GetServiceSetting", "vpc-lattice:GetAccessLogSubscription", "vpc-lattice:GetService", "vpc-lattice:GetServiceNetwork", "vpc-lattice:GetTargetGroup", "vpc-lattice:ListAccessLogSubscriptions", "vpc-lattice:ListServiceNetworks", "vpc-lattice:ListServices", "vpc-lattice:ListTagsForResource", "vpc-lattice:ListTargetGroups", and "vpc-lattice:ListTargets"		

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan "aoss:BatchGetCollection," "aoss:BatchGetLifecyclePolicy," "aoss:BatchGetVpcEndpoint," "aoss:GetAccessPolicy," "aoss:GetSecurityConfig," "aoss:GetSecurityPolicy," "aoss:ListAccessPolicies," "aoss:ListCollections," "aoss:ListLifecyclePolicies," "aoss:ListSecurityConfigs," "aoss:ListSecurityPolicies," "aoss:ListVpcEndpoints," "appstream:DescribeAppBlockBuilders," "backup:GetRestoreTestingPlan," "backup:GetRestoreTestingSelection", "backup:ListRestoreTestingPlans," "backup:ListRestoreTestingSelections," "cloudTrail:GetChannel, "cloudTrail:ListChannels," "glue:GetTrigger," "glue:ListTriggers, "imagebuilder:GetLifecyclePolicy," "imagebuilder:ListLifecyclePolicies," "iot:DescribeBillingGroup," "iot:ListBillingGroups," "ivs:GetEncoderConfiguration," "ivs:GetPlaybackRestrictionPolicy," "ivs:GetStage," "ivs:GetStorageConfiguration," "ivs:ListEncoderConfigurations,"	Kebijakan ini sekarang mendukung izin tambahan untuk Amazon OpenSearch Service Severless AppStream , Amazon,,, AWS Backup, EC2 Image Builder AWS CloudTrail AWS Glue AWS IoT, Amazon Interactive Video Service (Amazon IVS), AWS Elemental MediaConnect,,, AWS Elemental MediaTailor, AWS HealthOmics dan Amazon Scheduler. EventBridge	September 16, 2024

Perubahan	Deskripsi	Tanggal
"ivs:ListPlaybackRestrictionPolicies," "ivs:ListStages," "ivs:ListStorageConfigurations," "mediaconnect:DescribeBridge", "mediaconnect:DescribeGatewa," "mediaconnect:ListBridges," "mediaconnect:ListGateways", "mediatailor:DescribeChannel," "mediatailor:DescribeLiveSource," "mediatailor:DescribeSourceLocation," "mediatailor:DescribeVodSource", "mediatailor:ListChannels," "mediatailor:ListLiveSources", "mediatailor:ListSourceLocations," "mediatailor:ListVodSources," "omics:GetWorkflow," "omics:ListWorkflows," "scheduler:GetSchedule," and "scheduler:ListSchedules"		

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan "aoss:BatchGetCollection," "aoss:BatchGetLifecyclePolicy," "aoss:BatchGetVpcEndpoint," "aoss:GetAccessPolicy," "aoss:GetSecurityConfig," "aoss:GetSecurityPolicy," "aoss:ListAccessPolicies," "aoss:ListCollections," "aoss:ListLifecyclePolicies," "aoss:ListSecurityConfigs," "aoss:ListSecurityPolicies," "aoss:ListVpcEndpoints," "appstream:DescribeAppBlockBuilders," "backup:GetRestoreTestingPlan," "backup:GetRestoreTestingSelection", "backup:ListRestoreTestingPlans," "backup:ListRestoreTestingSelections," "cloudTrail:GetChannel, "cloudTrail:ListChannels," "glue:GetTrigger," "glue:ListTriggers, "imagebuilder:GetLifecyclePolicy," "imagebuilder:ListLifecyclePolicies," "iot:DescribeBillingGroup, " "iot:ListBillingGroups," "ivs:GetEncoderConfiguration, " "ivs:GetPlaybackRestrictionPolicy," "ivs:GetStage," "ivs:GetStorageConfiguration, " "ivs:ListEncoderConfigurati	Kebijakan ini sekarang mendukung izin tambahan untuk Amazon OpenSearch Service Severless AppStream , Amazon,,, AWS Backup, EC2 Image Builder AWS CloudTrail AWS Glue AWS IoT, Amazon Interactive Video Service (Amazon IVS), AWS Elemental MediaConnect,,, AWS Elemental MediaTailor, AWS HealthOmics dan Amazon Scheduler. EventBridge	September 16, 2024

Perubahan	Deskripsi	Tanggal
ons," "ivs:ListPlaybackRestrictionPolicies," "ivs:ListStages," "ivs:ListStorageConfigurations," "mediaconnect:DescribeBridge", "mediaconnect:DescribeGatewa," "mediaconnect:ListBridges," "mediaconnect:ListGateways", "mediatailor:DescribeChannel," "mediatailor:DescribeLiveSource," "mediatailor:DescribeSourceLocation," "mediatailor:DescribeVodSource", "mediatailor:ListChannels," "mediatailor:ListLiveSources", "mediatailor:ListSourceLocations," "mediatailor:ListVodSources," "omics:GetWorkflow," "omics:ListWorkflows," "scheduler:GetSchedule," and "scheduler:ListSchedules"		
AWS_ConfigRole— Tambahkan "elasticfilesystem:DescribeTags," "redshift:DescribeTags," and "ssm-sap:ListTagsForResource"	Kebijakan ini sekarang mendukung izin tambahan untuk Amazon Elastic File System (Amazon EFS), Amazon Manajer Sistem AWS untuk SAP Redshift, dan.	Juni 17, 2024
AWSConfigServiceRolePolicy— Tambahkan "elasticfilesystem:DescribeTags," "redshift:DescribeTags," and "ssm-sap:ListTagsForResource"	Kebijakan ini sekarang mendukung izin tambahan untuk Amazon Elastic File System (Amazon EFS), Amazon Manajer Sistem AWS untuk SAP Redshift, dan.	Juni 17, 2024

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan "aps:DescribeAlertManagerDefinition," "cloudwatch:DescribeAlarmsForMetric," "cognito-identity:DescribeIdentityPool, "cognito-identity:GetPrincipalTagAttributeMap," "elasticache:DescribeCacheSecurityGroups," "elasticache:DescribeUserGroups," "elasticache:DescribeUsers," "elasticache:DescribeGlobalReplicationGroups," "fsx:DescribeDataRepositoryAssociations," "glue:GetDatabase," "glue:GetDatabases," "iam:ListUsers," "lambda:GetLayerVersion," "lambda:ListLayers," "lambda:ListLayerVersions," "ram:GetPermission," "ram:ListPermissionAssociations," "ram:ListPermissions," "ram:ListPermissionVersions," "redshift-serverless:GetNamespace," "redshift-serverless:GetWorkgroup," "redshift-serverless:ListNamespaces," "redshift-serverless:ListTagsForResource," "redshift-serverless:ListWorkgroups," "sagemaker:DescribeInferenceExperiment," "sagemaker:ListInferenceExperiments," and "sns:G	Kebijakan ini sekarang mendukung izin tambahan untuk Layanan Terkelola Amazon untuk Prometheus, Amazon, Amazon CloudWatch Cognito, Amazon, Amazon,, (AWS Identity and Access Management IAM) ElastiCache,, AWS Glue, FSx Amazon AWS RAM Redshift Tanpa Server, AWS Lambda Amazon AI, dan Layanan Notifikasi Sederhana Amazon (Amazon SNS). SageMaker	Februari 22, 2024

Perubahan	Deskripsi	Tanggal
etSMSSandboxAccountStatus"		

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan "aps:DescribeAlertManagerDefinition," "cloudwatch:DescribeAlarmsForMetric," "cognito-identity:DescribeIdentityPool, "cognito-identity:GetPrincipalTagAttributeMap," "elasticache:DescribeCacheSecurityGroups," "elasticache:DescribeUserGroups," "elasticache:DescribeUsers," "elasticache:DescribeGlobalReplicationGroups," "fsx:DescribeDataRepositoryAssociations," "glue:GetDatabase," "glue:GetDatabases," "iam:ListUsers," "lambda:GetLayerVersion," "lambda:ListLayers," "lambda:ListLayerVersions," "ram:GetPermission," "ram:ListPermissionAssociations," "ram:ListPermissions," "ram:ListPermissionVersions," "redshift-serverless:GetNamespace," "redshift-serverless:GetWorkgroup," "redshift-serverless:ListNamespaces," "redshift-serverless:ListTagsForResource," "redshift-serverless:ListWorkgroups," "sagemaker:DescribeInferenceExperiment," "sagemaker:ListInferenceExperiments," and "sns:G	Kebijakan ini sekarang mendukung izin tambahan untuk Layanan Terkelola Amazon untuk Prometheus, Amazon, Amazon CloudWatch Cognito, Amazon, Amazon,, (AWS Identity and Access Management IAM) ElastiCache,, AWS Glue, FSx Amazon AWS RAM Redshift Tanpa Server, AWS Lambda Amazon AI, dan Layanan Notifikasi Sederhana Amazon (Amazon SNS). SageMaker	Februari 22, 2024

Perubahan	Deskripsi	Tanggal
etSMSSandboxAccountStatus"		
AWSConfigUserAccess—AWS Config mulai melacak perubahan untuk kebijakan AWS terkelola ini	Kebijakan ini menyediakan akses untuk digunakan AWS Config, termasuk mencari berdasarkan tag pada sumber daya dan membaca semua tag. Ini tidak memberikan izin untuk mengkonfigurasi AWS Config, yang membutuhkan hak administratif.	Februari 22, 2024
AWS_ConfigRole—Tambahkan "appconfig:GetExtensionAssociation," "appconfig:ListExtensionAssociations," "aps:DescribeLoggingConfiguration," "dms:DescribeReplicationTaskAssessmentRuns," "iam:GetOpenIDConnectProvider," "iam:ListOpenIDConnectProviders," "kafka:DescribeVpcConnection," "kafka:GetClusterPolicy," "kafka:ListVpcConnections," "logs:DescribeMetricFilters," "organizations:ListDelegatedAdministrators," "s3:GetBucketPolicyStatus," "s3express:GetBucketPolicy," and "s3express:ListAllMyDirectoryBuckets"	Kebijakan ini sekarang mendukung izin tambahan untuk AWS AppConfig, Amazon Managed Service for Prometheus, () AWS Database Migration Service ,AWS DMS(AWS Identity and Access Management) IAM, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Logs, dan Amazon Simple Storage Service (CloudWatch Amazon S3). AWS Organizations	Desember 5, 2023

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan "appconfig:GetExtensionAssociation," "appconfig:ListExtensionAssociations," "aps:DescribeLoggingConfiguration," "dms:DescribeReplicationTaskAssessmentRuns," "iam:GetOpenIDConnectProvider," "iam:ListOpenIDConnectProviders," "kafka:DescribeVpcConnection," "kafka:GetClusterPolicy," "kafka:ListVpcConnections," "logs:DescribeMetricFilters," "organizations:ListDelegatedAdministrators," "s3:GetBucketPolicyStatus," "s3express:GetBucketPolicy," and "s3express:ListAllMyDirectoryBuckets"	Kebijakan ini sekarang mendukung izin tambahan untuk AWS AppConfig, Amazon Managed Service for Prometheus, () AWS Database Migration Service ,AWS DMS(AWS Identity and Access Management) IAM, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Logs, dan Amazon Simple Storage Service (CloudWatch Amazon S3). AWS Organizations	5 Desember 2023

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan "backup:DescribeProtectedResource," "cognito-identity:GetIdentityPoolRoles," "cognito-identity:ListIdentityPools," "cognito-identity:ListTagsForResource," "cognito-idp:DescribeIdentityProvider," "cognito-idp:DescribeResourceServer," "cognito-idp:DescribeUserPool," "cognito-idp:DescribeUserPoolClient," "cognito-idp:DescribeUserPoolDomain," "cognito-idp:GetGroup," "cognito-idp:GetUserPoolMfaConfig," "cognito-idp:ListGroups," "cognito-idp:ListIdentityProviders," "cognito-idp:ListResourceServers," "cognito-idp:ListUserPoolClients," "cognito-idp:ListUserPools," "cognito-idp:ListTagsForResource," "connect:DescribeEvaluationForm," "connect:DescribeInstanceStorageConfig," "connect:DescribePrompt," "connect:DescribeRule," "connect:DescribeUser," "connect:GetTaskTemplate," "connect:ListApprovedOrigins," "connect:ListEvaluationForms," "connect:ListInstanceStorageConfigs," "connect	Kebijakan ini sekarang mendukung izin tambahan untuk Amazon Cognito, Amazon Connect, Amazon EMR,, Amazon MemoryDB, AWS Ground Station, Amazon AWS Mainframe Modernization, Amazon, Amazon Relational Database QuickSight Service (Amazon RDS) AWS Organizations, Amazon Redshift, Amazon Route 53,, dan. AWS Service Catalog AWS Transfer Family	17 November 2023

Perubahan	Deskripsi	Tanggal
:ListIntegrationAssociations," "connect:ListPrompts," "connect:ListRules," "connect:ListSecurityKeys," "connect:ListTagsForResource," "connect:ListTaskTemplates," "connect:ListUsers," "emr-containers:DescribeVirtualCluster," "emr-containers:ListVirtualClusters," "emr-serverless:GetApplication," "emr-serverless:ListApplications," "groundstation:GetDataflowEndpointGroup," "groundstation:ListDataflowEndpointGroups," "m2:GetEnvironment," "m2:ListEnvironments," "m2:ListTagsForResource," "memorydb:DescribeAcls," "memorydb:DescribeClusters," "memorydb:DescribeParameterGroups," "memorydb:DescribeParameters," "memorydb:DescribeSubnetGroups," "organizations:ListRoots," "quicksight:DescribeAccountSubscription," "quicksight:DescribeDataSetRefreshProperties," "rds:DescribeEngineDefaultClusterParameters," "redshift:DescribeEndpointAccess," "redshift:DescribeEndpointAuthorization," "route53:GetChange," "route53:ListCid		

Perubahan	Deskripsi	Tanggal
rBlocks," "route53:ListCidrLocations," "serviceCatalog:DescribePortfolioShares," "transfer:DescribeProfile," and "transfer:ListProfiles"		
AWS_ConfigRole—Tambahkan "Sid": "AWSConfigServiceRolePolicyStatementID," "Sid": "AWSConfigSLRLogStatementID," "Sid": "AWSConfigSLRLogEventStatementID," and "Sid": "AWSConfigSLRApiGatewayStatementID"	Kebijakan ini sekarang menambahkan pengidentifikasi keamanan (SID) untuk`AWSConfigServiceRolePolicyStatementID` ,, `AWSConfigSLRLogStatementID` `AWSConfigSLRLogEventStatementID` , dan`AWSConfigSLRApiGatewayStatementID` .	17 November 2023

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan "backup:DescribeProtectedResource," "cognito-identity:GetIdentityPoolRoles," "cognito-identity:ListIdentityPools," "cognito-identity:ListTagsForResource," "cognito-idp:DescribeIdentityProvider," "cognito-idp:DescribeResourceServer," "cognito-idp:DescribeUserPool," "cognito-idp:DescribeUserPoolClient," "cognito-idp:DescribeUserPoolDomain," "cognito-idp:GetGroup," "cognito-idp:GetUserPoolMfaConfig," "cognito-idp:ListGroups," "cognito-idp:ListIdentityProviders," "cognito-idp:ListResourceServers," "cognito-idp:ListUserPoolClients," "cognito-idp:ListUserPools," "cognito-idp:ListTagsForResource," "connect:DescribeEvaluationForm," "connect:DescribeInstanceStorageConfig," "connect:DescribePrompt," "connect:DescribeRule," "connect:DescribeUser," "connect:GetTaskTemplate," "connect:ListApprovedOrigins," "connect:ListEvaluationForms," "connect:ListInstanceStorageConfigs," "connect	Kebijakan ini sekarang mendukung izin tambahan untuk Amazon Cognito, Amazon Connect, Amazon EMR,, Amazon MemoryDB, AWS Ground Station, Amazon AWS Mainframe Modernization, Amazon, Amazon Relational Database QuickSight Service (Amazon RDS) AWS Organizations, Amazon Redshift, Amazon Route 53,, dan. AWS Service Catalog AWS Transfer Family	17 November 2023

Perubahan	Deskripsi	Tanggal
:ListIntegrationAssociations," "connect:ListPrompts," "connect:ListRules," "connect:ListSecurityKeys," "connect:ListTagsForResource," "connect:ListTaskTemplates," "connect:ListUsers," "emr-containers:DescribeVirtualCluster," "emr-containers:ListVirtualClusters," "emr-serverless:GetApplication," "emr-serverless:ListApplications," "groundstation:GetDataflowEndpointGroup," "groundstation:ListDataflowEndpointGroups," "m2:GetEnvironment," "m2:ListEnvironments," "m2:ListTagsForResource," "memorydb:DescribeAcls," "memorydb:DescribeClusters," "memorydb:DescribeParameterGroups," "memorydb:DescribeParameters," "memorydb:DescribeSubnetGroups," "organizations:ListRoots," "quicksight:DescribeAccountSubscription," "quicksight:DescribeDataSetRefreshProperties," "rds:DescribeEngineDefaultClusterParameters," "redshift:DescribeEndpointAccess," "redshift:DescribeEndpointAuthorization," "route53:GetChange," "route53:ListCid		

Perubahan	Deskripsi	Tanggal
rBlocks," "route53:ListCidrLocations," "serviceCatalog:DescribePortfolioShares," "transfer:DescribeProfile," and "transfer:ListProfiles"		
AWSConfigServiceRolePolicy— Tambahkan "Sid": "AWSConfigServiceRolePolicyStatementID," "Sid": "AWSConfigSLRLogStatementID," "Sid": "AWSConfigSLRLogEventStatementID," and "Sid": "AWSConfigSLRApiGatewayStatementID"	Kebijakan ini sekarang menambahkan pengidentifikasi keamanan (SID) untuk`AWSConfigServiceRolePolicyStatementID` ,, `AWSConfigSLRLogStatementID` `AWSConfigSLRLogEventStatementID` , dan`AWSConfigSLRApiGatewayStatementID` .	17 November 2023

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan "acm-pca: GetCertificateAuthorityCertificate," "appmesh:DescribeMesh," "appmesh:ListGatewayRoutes," "connect:DescribeInstance," "connect:DescribeQuickConnect," "connect:ListQuickConnects," "ecs:DescribeCapacityProviders," "evidently:GetSegment," "evidently:ListSegments," "grafana:DescribeWorkspace," "grafana:DescribeWorkspaceAuthentication," "grafana:DescribeWorkspaceConfiguration," "grafana:DescribeWorkspaceConfiguration," "guardduty:GetMemberDetectors," "inspector2:BatchGetAccountStatus," "inspector2:GetDelegatedAdminAccount," "inspector2:ListMembers," "iot:DescribeCACertificate," "iot:ListCACertificates," "iot:ListTagsForResource," "iottwinmaker:GetSyncJob," "iottwinmaker:ListSyncJobs," "kafka:ListTagsForResource," "kafkaconnect:DescribeConnector," "kafkaconnect:ListConnectors," "lambda:GetCodeSigningConfig," "lambda:ListCodeSi	Kebijakan ini sekarang mendukung izin tambahan untuk AWS Private CA,, Amazon Connect AWS App Mesh, Amazon Elastic Container Service (Amazon ECS), Amazon CloudWatch Terbukti, Amazon Managed Grafana, Amazon, Amazon Inspector,, GuardDuty, Amazon AWS IoT Managed AWS IoT TwinMaker Streaming untuk Apache Kafka (Amazon MSK),,,,, dan Amazon AI. AWS Lambda AWS Network Manager AWS Organizations SageMaker	4 Oktober 2023

Perubahan	Deskripsi	Tanggal
gningConfigs," "lambda:ListTags," "networkmanager:GetConnectPeer," "organizations:DescribeOrganization," "organizations:ListTargetsForPolicy," "sagemaker:DescribeDataQualityJob," "sagemaker:DescribeModelExplainabilityJob," "sagemaker:ListDataQualityJob," and "sagemaker:ExplainabilityJob"		

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan "acm-pca:GetCertificateAuthorityCertificate," "appmesh:DescribeMesh," "appmesh:ListGatewayRoutes," "connect:DescribeInstance," "connect:DescribeQuickConnect," "connect:ListQuickConnects," "ecs:DescribeCapacityProviders," "evidently:GetSegment," "evidently:ListSegments," "grafana:DescribeWorkspace," "grafana:DescribeWorkspaceAuthentication," "grafana:DescribeWorkspaceConfiguration," "grafana:DescribeWorkspaceConfiguration," "guardduty:GetMemberDetectors," "inspector2:BatchGetAccountStatus," "inspector2:GetDelegatedAdminAccount," "inspector2:ListMembers," "iot:DescribeCACertificate," "iot:ListCACertificates," "iot:ListTagsForResource," "iottwinmaker:GetSyncJob," "iottwinmaker:ListSyncJobs," "kafka:ListTagsForResource," "kafkaconnect:DescribeConnector," "kafkaconnect:ListConnectors," "lambda:GetCodeSigningConfig," "lambda:ListCodeSi	Kebijakan ini sekarang mendukung izin tambahan untuk AWS Private CA,, Amazon Connect AWS App Mesh, Amazon Elastic Container Service (Amazon ECS), Amazon CloudWatch Terbukti, Amazon Managed Grafana, Amazon, Amazon Inspector,, GuardDuty, Amazon AWS IoT Managed AWS IoT TwinMaker Streaming untuk Apache Kafka (Amazon MSK),,,,, dan Amazon AI. AWS Lambda AWS Network Manager AWS Organizations SageMaker	4 Oktober 2023

Perubahan	Deskripsi	Tanggal
gningConfigs," "lambda:ListTags," "networkmanager:GetConnectPeer," "organizations:DescribeOrganization," "organizations:ListTargetsForPolicy," "sagemaker:DescribeDataQualityJob," "sagemaker:DescribeModelExplainabilityJob," "sagemaker:ListDataQualityJob," and "sagemaker:ExplainabilityJob"		
AWSConfigServiceRolePolicy— Hapus "ssm:GetParameter"	Kebijakan ini sekarang menghapus izin untuk AWS Systems Manager (Systems Manager).	September 6, 2023

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan "appmesh: DescribeGatewayRoute","appstream:DescribeStacks", "aps:ListTagsForResource", "cloudfront:GetFunction", "cloudfront:GetOriginAccessControl", "cloudfront:ListFunctions", "cloudfront:ListOriginAccessControls", "codeartifact:ListPackages", "codeartifact:ListPackageVersions", "codebuild:BatchGetReportGroups", "codebuild:ListReportGroups", "connect:ListInstanceAttributes", "connect:ListInstances", "glue:GetPartition", "glue:GetPartitions", "guardduty:GetAdministratorAccount", "iam:ListInstanceProfileTags", "inspector2:ListFilters", "iot:DescribeJobTemplate", "iot:DescribeProvisioningTemplate", "iot:ListJobTemplates", "iot:ListProvisioningTemplates", "iottwinmaker:GetComponentType", "iottwinmaker:ListComponentTypes", "iotwireless:GetFuotaTask", "iotwireless:GetMulticastGroup", "iotwireless:ListFuotaTasks", "iotwireless:ListMulticastGroups", "kafka:ListScramSe	Kebijakan ini sekarang mendukung izin tambahan untuk AWS App Mesh,, Amazon, AWS CloudFormation, Amazon Connect CloudFront AWS CodeArtifact, AWS CodeBuild, Amazon, AWS Identity and Access Management (IAM) AWS Glue GuardDuty, Amazon Inspector AWS IoT,,,, Amazon Managed Streaming untuk Apache Kafka AWS IoT TwinMaker AWS IoT Wireless, Amazon AWS Elemental MediaConnect AWS Network Manager Macie,,,, Amazon Route 53 AWS Organizations Penjelajah Sumber Daya AWS, Amazon Simple Storage Service (Amazon S3), dan Amazon Simple Layanan Pemberitahuan (Amazon SNS).	28 Juli 2023

Perubahan	Deskripsi	Tanggal
crets", "macie2:ListTagsForResource", "mediaconnect:ListTagsForResource", "networkmanager:GetConnectPeer", "networkmanager:ListConnectPeers", "organizations:DescribeEffectivePolicy", "organizations:DescribeResourcePolicy", "resource-explorer-2:GetIndex", "resource-explorer-2:ListIndexes", "resource-explorer-2:ListTagsForResource", "route53:ListCidrCollections", "s3:GetMultiRegionAccessPointPolicy", "s3:GetMultiRegionAccessPointPolicyStatus", and "sns:GetDataProtectionPolicy"		

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan "appmesh:DescribeGatewayRoute", "appstream:DescribeStacks", "aps:ListTagsForResource", "cloudfront:GetFunction", "cloudfront:GetOriginAccessControl", "cloudfront:ListFunctions", "cloudfront:ListOriginAccessControls", "codeartifact:ListPackages", "codeartifact:ListPackageVersions", "codebuild:BatchGetReportGroups", "codebuild:ListReportGroups", "connect:ListInstanceAttributes", "connect:ListInstances", "glue:GetPartition", "glue:GetPartitions", "guardduty:GetAdministratorAccount", "iam:ListInstanceProfileTags", "inspector2:ListFilters", "iot:DescribeJobTemplate", "iot:DescribeProvisioningTemplate", "iot:ListJobTemplates", "iot:ListProvisioningTemplates", "iottwinmaker:GetComponentType", "iottwinmaker:ListComponentTypes", "iotwireless:GetFuotaTask", "iotwireless:GetMulticastGroup", "iotwireless:ListFuotaTasks", "iotwireless:ListMulticas	Kebijakan ini sekarang mendukung izin tambahan untuk AWS App Mesh, Amazon AppStream 2.0,, Amazon,, AWS CloudFormation, Amazon Connect CloudFront, AWS CodeArtifact AWS CodeBuild, Amazon, AWS Identity and Access Management (IAM) AWS Glue GuardDuty, Amazon Inspector,,,, Amazon Managed Streaming untuk Apache Kafka AWS IoT AWS IoT TwinMaker AWS IoT Wireless, Amazon AWS Elemental MediaConnect AWS Network Manager Macie,,,, Amazon Route 53 AWS Organizations Penjelajah Sumber Daya AWS, Amazon Simple Storage Service (Amazon S3), Amazon Simple Notification Service (Amazon SNS), dan Amazon Systems Manager (SSM). EC2	28 Juli 2023

Perubahan	Deskripsi	Tanggal
tGroups", "kafka:ListScramSecrets", "macie2:ListTagsForResource", "mediaconnect:ListTagsForResource", "networkmanager:GetConnectPeer", "networkmanager:ListConnectPeers", "organizations:DescribeEffectivePolicy", "organizations:DescribeResourcePolicy", "resource-explorer-2:GetIndex", "resource-explorer-2:ListIndexes", "resource-explorer-2:ListTagsForResource", "route53:ListCidrCollections", "s3:GetMultiRegionAccessPointPolicy", "s3:GetMultiRegionAccessPointPolicyStatus", "sns:GetDataProtectionPolicy", "ssm:DescribeParameters", "ssm:GetParameter", and "ssm:ListTagsForResource"		

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan "amplify: GetBranch", "amplify:ListBranches", "app-integrations:GetEventIntegration", "app-integrations:ListEventIntegrationAssociations", "app-integrations:ListEventIntegrations", "appmesh: DescribeRoute", "appmesh:ListRoutes", "aps:ListRuleGroupsNamespaces", "athena:GetPreparedStatement", "athena:ListPreparedStatements", "batch:DescribeSchedulingPolicies", "batch:ListSchedulingPolicies", "cloudformation:ListTypes", "cloudtrail:ListTrails", "codeartifact:ListDomains", "codeguru-profiler:DescribeProfilingGroup", "codeguru-profiler:GetNotificationConfiguration", "codeguru-profiler: GetPolicy", "codeguru-profiler:ListProfilingGroups", "ds:DescribeDomainControllers", “dynamodb:DescribeTableReplicaAutoScaling" "dynamodb:DescribeTimeToLive", "ec2:DescribeTrafficMirrorFilters", "evidently:GetLaunch", "evidently:ListLaunches",	Kebijakan ini sekarang mendukung izin tambahan untuk AWS Amplify, Amazon Connect,, Amazon Managed Service untuk Prometheus AWS App Mesh, Amazon AWS Batch Athena,,,,, Amazon,, Amazon DynamoDB AWS CloudFormation AWS CloudTrail AWS CodeArtifact CodeGuru, Amazon Elastic Compute Cloud (Amazon) AWS Directory Service, Amazon Terbukti AWS Organizations,, Amazon Forecast, ,, (AWS IoT Greengrass IAM EC2), CloudWatch Amazon Managed Streaming untuk Apache Kafka Apache (Amazon MSK) AWS Ground Station, AWS Identity and Access Management Amazon Lightsail, Log Amazon,,, Amazon Pinpoint, Amazon Virtual Private Cloud (CloudWatch AWS Elemental MediaConnect AWS Elemental MediaTailor Amazon VPC), Amazon Personalisasi, Amazon,, Layanan Penyimpanan Sederhana QuickSight Amazon AWS Migration Hub	13 Juni 2023

Perubahan	Deskripsi	Tanggal
"forecast:DescribeDatasetGroup", "forecast:ListDatasetGroups", "greengrass:DescribeComponent", "greengrass:GetComponent", "greengrass:ListComponents", "greengrass:ListComponentVersions", "groundstation:GetMissionProfile", "groundstation:ListMissionProfiles", "iam:ListGroups", "iam:ListRoles", "kafka:DescribeConfiguration", "kafka:DescribeConfigurationRevision", "kafka:ListConfigurations", "lightsail:GetRelationalDatabases" "logs:ListTagsLogGroup", "mediaconnect:DescribeFlow", "mediaconnect:ListFlows", "mediatailor:GetPlaybackConfiguration", "mediatailor:ListPlaybackConfigurations", "mobiletargeting:GetApplicationSettings", "mobiletargeting:GetEmailTemplate", "mobiletargeting:GetEventStream", "mobiletargeting:ListTemplates", "networkmanager:GetCustomerGatewayAssociations", "networkmanager:GetLinkAssociations", "organizations:DescribeAccount", "organizations:DescribeOrganizationalUnit", "organ	Refactor Spaces(Amazon S3) Simple Storage Service SageMaker S3), Amazon AI,. AWS Transfer Family	

Perubahan	Deskripsi	Tanggal
izations:ListAccounts", "organizations:ListAccounts ForParent", "organizations:L istOrganizationalUnitsForPa rent", "organizations:ListTa gsForResource", "personal ize:DescribeDataset", "perso nalize:DescribeDatasetGroup", "personalize:DescribeSchema ", "personalize:DescribeSolu tion", "personalize:ListD atasetGroups", "personalize: ListDatasetImportJobs", "personalize:ListDatasets", "personalize:ListSchemas", "personalize:ListSolutions", "personalize:ListTagsForRe source", "quicksight:ListTe mplates", "refactor-spaces:G etEnvironment", "refactor -spaces:GetService", "refactor-spaces:ListAppl ications", "refactor-spaces: ListEnvironments", "refactor -spaces:ListServices", "s3:GetAccessPointPolic yStatusForObjectLambda", "sagemaker:DescribeDe viceFleet", "sagemake r:DescribeFeatureGroup", "sa gemaker:ListDeviceFleets", "sagemaker:ListFeatureGroup s", "sagemaker:ListModels",		

Perubahan	Deskripsi	Tanggal
and "transfer:ListTags ForResource"		

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan "amplify:GetBranch", "amplify:ListBranches", "app-integrations:GetEventIntegration", "app-integrations:ListEventIntegrationAssociations", "app-integrations:ListEventIntegrations", "appmesh:DescribeRoute", "appmesh:ListRoutes", "aps:ListRuleGroupsNamespaces", "athena:GetPreparedStatement", "athena:ListPreparedStatements", "batch:DescribeSchedulingPolicies", "batch:ListSchedulingPolicies", "cloudformation:ListTypes", "cloudtrail:ListTrails", "codeartifact:ListDomains", "codeguru-profiler:DescribeProfilingGroup", "codeguru-profiler:GetNotificationConfiguration", "codeguru-profiler:GetPolicy", "codeguru-profiler:ListProfilingGroups", "ds:DescribeDomainControllers", "dynamodb:DescribeTableReplicaAutoScaling", "dynamodb:DescribeTimeToLive", "ec2:DescribeTrafficMirrorFilters", "evidently:GetLaunch", "evidently:ListLaunches", "forecast:DescribeDa	Kebijakan ini sekarang mendukung izin tambahan untuk AWS Amplify, Amazon Connect,, Amazon Managed Service untuk Prometheus AWS App Mesh, Amazon AWS Batch Athena,,,,, Amazon,, Amazon DynamoDB AWS CloudFormation AWS CloudTrail AWS CodeArtifact CodeGuru, Amazon Elastic Compute Cloud (Amazon) AWS Directory Service, Amazon Terbukti AWS Organizations,, Amazon Forecast, ,, (AWS IoT Greengrass IAM EC2), CloudWatch Amazon Managed Streaming untuk Apache Kafka Apache (Amazon MSK) AWS Ground Station, AWS Identity and Access Management Amazon Lightsail, Log Amazon,,, Amazon Pinpoint, Amazon Virtual Private Cloud (CloudWatch AWS Elemental MediaConnect AWS Elemental MediaTailor Amazon VPC), Amazon Personalisasi, Amazon,, Layanan Penyimpanan Sederhana QuickSight Amazon AWS Migration Hub	13 Juni 2023

Perubahan	Deskripsi	Tanggal
tasetGroup", "forecast :ListDatasetGroups", "greengrass:DescribeComponent", "greengrass:GetComponent", "greengrass:ListComponents", "greengrass:ListComponentVersions", "groundstation:GetMissionProfile", "groundstation:ListMissionProfiles", "iam:ListGroups", "iam:ListRoles", "kafka:DescribeConfiguration", "kafka:DescribeConfigurationRevision", "kafka:ListConfigurations", "lightsail:GetRelationalDatabases", "logs:ListTagsLogGroup", "mediaconnect:DescribeFlow", "mediaconnect:ListFlows", "mediatailor:GetPlaybackConfiguration", "mediatailor:ListPlaybackConfigurations", "mobiletargeting:GetApplicationSettings", "mobiletargeting:GetEmailTemplate", "mobiletargeting:GetEventStream", "mobiletargeting:ListTemplates", "networkmanager:GetCustomerGatewayAssociations", "networkmanager:GetLinkAssociations", "organizations:DescribeAccount", "organizations:DescribeOrganizationalUnit", "organizations:ListAccounts",	Refactor Spaces(Amazon S3) Simple Storage Service SageMaker S3), Amazon AI,. AWS Transfer Family	

Perubahan	Deskripsi	Tanggal
"organizations:ListAccounts ForParent", "organizations:L istOrganizationalUnitsForPa rent", "organizations:ListTa gsForResource", "personal ize:DescribeDataset", "perso nalize:DescribeDatasetGroup", "personalize:DescribeSchema ", "personalize:DescribeSolu tion", "personalize:ListD atasetGroups", "personalize: ListDatasetImportJobs", "personalize:ListDatasets", "personalize:ListSchemas", "personalize:ListSolutions", "personalize:ListTagsForRe source", "quicksight:ListTe mplates", "refactor-spaces:G etEnvironment", "refactor -spaces:GetService", "refactor-spaces:ListAppl ications", "refactor-spaces: ListEnvironments", "refactor -spaces:ListServices", "s3:GetAccessPointPolic yStatusForObjectLambda", "sagemaker:DescribeDe viceFleet", "sagemake r:DescribeFeatureGroup", "sa gemaker:ListDeviceFleets", "sagemaker:ListFeatureGroup s", "sagemaker:ListModels", and "transfer:ListTags ForResource"		

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan amplify:GetApp, amplify:ListApps, appmesh:DescribeVirtualGateway, appmesh:DescribeVirtualNode, appmesh:DescribeVirtualRouter, appmesh:DescribeVirtualService, appmesh:ListMeshes, appmesh:ListTagsForResource, appmesh:ListVirtualGateways, appmesh:ListVirtualNodes, appmesh:ListVirtualRouters, appmesh:ListVirtualServices, apprunner:DescribeVpcConnector, apprunner:ListVpcConnectors, cloudformation:ListTypes, cloudfront:ListResponseHeadersPolicies, codeartifact:ListRepositories, ds:DescribeEventTopics, ds:ListLogSubscriptions, GetInstanceTypesFromInstanceRequirement ec2:GetManagedPrefixListEntries, kendra:DescribeIndex, kendra:ListIndices, kendra:ListTagsForResource, logs:DescribeDestinations, logs:GetDataProtectionPolicy, macie2:DescribeOrganizationConfiguration, macie2:GetAutomatedDiscoveryConfigurat	Kebijakan ini sekarang mendukung izin tambahan untuk Alur Kerja Terkelola Amazon untuk AWS Amplify,, , AWS App Runner Amazon AWS App Mesh CloudFront, AWS CodeArtifact Amazon Elastic Compute Cloud, Amazon Kendra, Amazon Macie, Amazon Route 53, Amazon SageMaker AI,, Amazon Pinpoint, AWS Transfer Family, AWS Resilience Hub, Amazon AWS Migration Hub, Directory Service, dan. CloudWatch AWS AWS WAF	13 April 2023

Perubahan	Deskripsi	Tanggal
ion, macie2:GetClassificationExportConfiguration, macie2:GetCustomDataIdentifier, macie2:GetFindingsPublicationConfiguration, macie2:ListCustomDataIdentifiers, mobiletargeting:GetEmailChannel, refactor-spaces:GetEnvironment, refactor-spaces:ListEnvironments, resiliencehub:ListTagsForResource, route53:GetDNSSEC, sagemaker:DescribeDomain, sagemaker:DescribeModelBiasJobDefinition, sagemaker:DescribeModelQualityJobDefinition, sagemaker:DescribePipeline, sagemaker:DescribeProject, sagemaker:ListDomains, sagemaker:ListModelBiasJobDefinitions, sagemaker:ListModelQualityJobDefinitions, sagemaker:ListPipelines, sagemaker:ListProjects, transfer:DescribeAgreement, transfer:DescribeCertificate, transfer:ListAgreements, transfer:ListCertificates, and waf-regional:ListLoggingConfigurations		

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan amplify:GetApp, amplify:ListApps, appmesh:DescribeVirtualGateway, appmesh:DescribeVirtualNode, appmesh:DescribeVirtualRouter, appmesh:DescribeVirtualService, appmesh:ListMeshes, appmesh:ListTagsForResource, appmesh:ListVirtualGateways, appmesh:ListVirtualNodes, appmesh:ListVirtualRouters, appmesh:ListVirtualServices, apprunner:DescribeVpcConnector, apprunner:ListVpcConnectors, cloudformation:ListTypes, cloudfront:ListResponseHeadersPolicies, codeartifact:ListRepositories, ds:DescribeEventTopics, ds:ListLogSubscriptions, ec2:GetInstanceTypesFromInstanceRequirement, ec2:GetManagedPrefixListEntries, kendra:DescribeIndex, kendra:ListIndices, kendra:ListTagsForResource, logs:DescribeDestinations, logs:GetDataProtectionPolicy, macie2:DescribeOrganizationConfiguration, macie2:GetAutomatedDiscoveryConfigurat	Kebijakan ini sekarang mendukung izin tambahan untuk Alur Kerja Terkelola Amazon untuk AWS Amplify,, , AWS App Runner Amazon AWS App Mesh CloudFront, AWS CodeArtifact Amazon Elastic Compute Cloud, Amazon Kendra, Amazon Macie, Amazon Route 53, Amazon SageMaker AI,, Amazon Pinpoint, AWS Transfer Family, AWS Resilience Hub, Amazon AWS Migration Hub, Directory Service, dan. CloudWatch AWS AWS WAF	13 April 2023

Perubahan	Deskripsi	Tanggal
ion, macie2:GetClassificationExportConfiguration, macie2:GetCustomDataIdentifier, macie2:GetFindingsPublicationConfiguration, macie2:ListCustomDataIdentifiers, mobiletargeting:GetEmailChannel, refactor-spaces:GetEnvironment, refactor-spaces:ListEnvironments, resiliencehub:ListTagsForResource, route53:GetDNSSEC, sagemaker:DescribeDomain, sagemaker:DescribeModelBiasJobDefinition, sagemaker:DescribeModelQualityJobDefinition, sagemaker:DescribePipeline, sagemaker:DescribeProject, sagemaker:ListDomains, sagemaker:ListModelBiasJobDefinitions, sagemaker:ListModelQualityJobDefinitions, sagemaker:ListPipelines, sagemaker:ListProjects, transfer:DescribeAgreement, transfer:DescribeCertificate, transfer:ListAgreements, transfer:ListCertificates, and waf-regional:ListLoggingConfigurations		

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan appflow:DescribeFlow, appflow:ListFlows, appflow:ListTagsForResource, apprunner:DescribeService, apprunner:ListServices, apprunner:ListTagsForResource, appstream:DescribeApplications, appstream:DescribeFleets, cloudfront:GetResponseHeadersPolicy, cloudwatch:ListTagsForResource, codeartifact:DescribeRepository, codeartifact:GetRepositoryPermissionsPolicy, codeartifact:ListTagsForResource, codecommit:GetRepository, codecommit:GetRepositoryTriggers, codecommit:ListRepositories, codecommit:ListTagsForResource, devicefarm:GetInstanceProfile, devicefarm:ListInstanceProfiles, devicefarm:ListProjects, evidently:GetProject, evidently:ListProjects, evidently:ListTagsForResource, forecast:DescribeDataset, forecast:ListDatasets, forecast:ListTagsForResource, groundstation:GetConfig, groundstation:ListConfigs, groundstation:ListTagsForRes	Kebijakan ini sekarang mendukung izin tambahan untuk Alur Kerja Terkelola Amazon untuk Amazon AppFlow,, AWS App Runner Amazon AppStream 2.0, Amazon, CloudWatch,,, CloudFront Amazon CloudWatch Terbukti AWS CodeArtifact AWS CodeCommit, AWS Device Farm Amazon Forecast,, AWS Identity and Access Management (IAM), AWS Ground Station, Amazon MemoryDB, AWS IoT Amazon Pinpoint,,, Amazon AWS Panorama Relational Database Service (AWS Network Manager Amazon RDS), Amazon Redshift, dan Amazon AI. SageMaker	30 Maret 2023

Perubahan	Deskripsi	Tanggal
ource, iam:GetInstancePro file, iam:GetSAMLProvider, iam:GetServerCertificate, iam:ListAccessKeys, iam:List Groups, iam:ListInstancePr ofiles, iam:ListMFADevices , iam:ListMFADeviceTags, iam:ListRoles, iam:ListS AMLProviders, iot:DescribeFl eetMetric, iot:ListFleetMetri cs, memorydb:Descri beUsers, memorydb:ListTags, mobiletargeting:GetApp, mobi letargeting:GetCampaigns, networkmanager:GetDevices, networkmanager:GetL inks, networkmanager:Get Sites, panorama:ListNodes, rds:DescribeDBProxyEndpoint s, redshift:DescribeSchedule dActions, sagemaker :DescribeAppImageConfig, sagemaker:DescribeIma ge, sagemaker:Describe ImageVersion, sagem aker:ListAppImageConfigs, sagemaker:ListImages, and sagemaker:ListImageVersions		

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan appflow:DescribeFlow, appflow:ListFlows, appflow:ListTagsForResource, apprunner:DescribeService, apprunner:ListServices, apprunner:ListTagsForResource, appstream:DescribeApplications, appstream:DescribeFleets, cloudformation:ListTypes, cloudfront:GetResponseHeadersPolicy, cloudfront:ListDistributions, cloudwatch:ListTagsForResource, codeartifact:DescribeRepository, codeartifact:GetRepositoryPermissionsPolicy, codeartifact:ListTagsForResource, codecommit:GetRepository, codecommit:GetRepositoryTriggers, codecommit:ListRepositories, codecommit:ListTagsForResource, devicefarm:GetInstanceProfile, devicefarm:ListInstanceProfiles, devicefarm:ListProjects, ec2:DescribeTrafficMirrorFilters, evidently:GetProject, evidently:ListProjects, evidently:ListTagsForResource, forecast:DescribeDataset, forecast:ListDatasets, forecast:ListTagsForResource,	Kebijakan ini sekarang mendukung izin tambahan untuk Alur Kerja Terkelola Amazon untuk Amazon AppFlow, Amazon AppStream 2.0,, AWS App Runner Amazon,,,, AWS CloudFormation Amazon, CloudWatch, AWS CodeArtifact AWS CodeCommit, CloudFront Amazon Elastic Compute Cloud (AWS Device Farm Amazon), Amazon CloudWatch Terbukti EC2, Amazon Forecast,, AWS Identity and Access Management (IAM), AWS Ground Station, Amazon MemoryDB, AWS IoT Amazon Pinpoint,,, Amazon AWS Panorama Relational Database Service (AWS Network Manager Amazon RDS), Amazon RedAmazon Redshift, dan Amazon AI. SageMaker	30 Maret 2023

Perubahan	Deskripsi	Tanggal
groundstation:GetConfig, groundstation:ListConfigs, groundstation:ListTagsForResource, iam:GetInstanceProfile, iam:GetSAMLProvider, iam:GetServerCertificate, iam:ListAccessKeys, iam:ListGroups, iam:ListInstanceProfiles, iam:ListMFADevices, iam:ListMFADeviceTags, iam:ListRoles, iam:ListSAMLProviders, iot:DescribeFleetMetric, iot:ListFleetMetrics, memorydb:DescribeUsers, memorydb:ListTags, mobiletargeting:GetApp, mobiletargeting:GetCampaigns, networkmanager:GetDevices, networkmanager:GetLinks, networkmanager:GetSites, panorama:ListNodes, rds:DescribeDBProxyEndpoints, redshift:DescribeScheduledActions, sagemaker:DescribeAppImageConfig, sagemaker:DescribeImage, sagemaker:DescribeImageVersion, sagemaker:ListAppImageConfigs, sagemaker:ListImages, and sagemaker:ListImageVersions		

Perubahan	Deskripsi	Tanggal
AWSConfigRulesExecutionRole— AWS Config mulai melacak perubahan untuk kebijakan AWS terkelola ini	Kebijakan ini memungkinkan AWS Lambda fungsi mengakses AWS Config API dan snapshot konfigurasi yang AWS Config dikirimkan secara berkala ke Amazon S3. Akses ini diperlukan oleh fungsi yang mengevaluasi perubahan konfigurasi untuk aturan Lambda AWS Kustom.	7 Maret 2023
AWSConfigRoleForOrganizations— AWS Config mulai melacak perubahan untuk kebijakan AWS terkelola ini	Kebijakan ini memungkinkan AWS Config untuk memanggil read-only AWS Organizations APIs.	7 Maret 2023
AWSConfigRemediationServiceRolePolicy— AWS Config mulai melacak perubahan untuk kebijakan AWS terkelola ini	Kebijakan ini memungkinkan AWS Config untuk memulihkan `NON_COMPLIANT` sumber daya atas nama Anda.	7 Maret 2023
AWSConfigServiceRolePolicy— Tambahkan auditmanager:GetAccountStatus	Kebijakan ini sekarang memberikan izin untuk mengembalikan status pendaftaran akun di AWS Audit Manager.	3 Maret 2023
AWS_ConfigRole— Tambahkan auditmanager:GetAccountStatus	Kebijakan ini sekarang memberikan izin untuk mengembalikan status pendaftaran akun di AWS Audit Manager.	3 Maret 2023

Perubahan	Deskripsi	Tanggal
AWSConfigMultiAccountSetupPolicy— AWS Config mulai melacak perubahan untuk kebijakan AWS terkelola ini	Kebijakan ini memungkinkan AWS Config untuk memanggil AWS layanan dan menyebarkan AWS Config sumber daya di seluruh organisasi dengan AWS Organizations.	27 Februari 2023

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:Ge	Kebijakan ini sekarang mendukung izin tambahan untuk Alur Kerja Terkelola Amazon untuk Apache Airflow, AWS IoT Amazon 2.0, Amazon CodeGuru Reviewer AppStream ,, Amazon Kinesis AWS HealthLake Video Streams, Amazon Application Recovery Controller (ARC), Amazon Elastic Compute Cloud (AWS Device Farm Amazon), Amazon Pinpoint, (IAM EC2), Amazon AWS Identity and Access Management , dan Log Amazon. GuardDuty CloudWatch	1 Februari 2023

Perubahan	Deskripsi	Tanggal
tTestGridProject, devicefarm:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar	Kebijakan ini sekarang mendukung izin tambahan untuk Alur Kerja Terkelola Amazon untuk Apache Airflow, AWS IoT Amazon 2.0, Amazon CodeGuru Reviewer AppStream ,, Amazon Kinesis AWS HealthLake Video Streams, Amazon Application Recovery Controller (ARC), Amazon Elastic Compute Cloud (AWS Device Farm Amazon), Amazon Pinpoint, (IAM EC2), Amazon AWS Identity and Access Management , dan Log Amazon. GuardDuty CloudWatch	1 Februari 2023

Perubahan	Deskripsi	Tanggal
m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		
ConfigConformsServiceRolePolicy— Perbarui config:DescribeConfigRules	Sebagai praktik terbaik keamanan, kebijakan ini sekarang menghapus izin tingkat sumber daya yang luas untuk. `config:DescribeConfigRules`	Januari 12, 2023

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, AWS Transfer Family devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager	Kebijakan ini sekarang mendukung izin tambahan untuk Amazon Managed Service untuk Prometheus AWS Audit Manager,,, (), AWS Device Farm Amazon Elastic Compute Cloud AWS Database Migration Service (Amazon AWS DMS), AWS Directory Service,, Amazon AWS IoT Lightsail,,, Amazon EC2, AWS Glue, Amazon Application Recovery Controller (ARC) AWS Elemental MediaPackage QuickSight, AWS Network Manager Amazon Simple Storage Service (AWS Resource Access Manager Amazon S3), dan Amazon Timestream.	Desember 15, 2022

Perubahan	Deskripsi	Tanggal
:GetTransitGatewayRegistrations, networkmanager:ListTagsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTa	Kebijakan ini sekarang mendukung izin tambahan untuk Amazon Managed Service untuk Prometheus AWS Audit Manager,,, (), AWS Device Farm Amazon Elastic Compute Cloud AWS Database Migration Service (Amazon AWS DMS), AWS Directory Service,, Amazon AWS IoT Lightsail,,, Amazon EC2, AWS Glue, Amazon Application Recovery Controller (ARC) AWS Elemental MediaPackage QuickSight, AWS Network Manager Amazon Simple Storage Service (AWS Resource Access Manager Amazon S3), dan Amazon Timestream.	Desember 15, 2022

Perubahan	Deskripsi	Tanggal
gsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan cloudformation:ListStackResources and cloudformation:ListStacks	Kebijakan ini sekarang memberikan izin untuk menampilkan deskripsi semua sumber daya dari AWS CloudFormation tumpukan tertentu dan mengembalikan informasi ringkasan untuk tumpukan yang statusnya cocok dengan yang ditentukan. StackStatusFilter	7 November 2022
AWS_ConfigRole— Tambahkan cloudformation:ListStackResources and cloudformation:ListStacks	Kebijakan ini sekarang memberikan izin untuk menampilkan deskripsi semua sumber daya dari AWS CloudFormation tumpukan tertentu dan mengembalikan informasi ringkasan untuk tumpukan yang statusnya cocok dengan yang ditentukan. StackStatusFilter	7 November 2022

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes,	Kebijakan ini sekarang mendukung izin tambahan untuk AWS Certificate Manager, Alur Kerja Terkelola Amazon untuk Apache Airflow,,, AWS Amplify Amazon Keyspaces, AWS AppConfig Amazon, Amazon Connect,, CloudWatch Amazon Elastic Compute Cloud (Amazon) AWS Glue DataBrew, Amazon EC2 Elastic Kubernetes Service (Amazon EKS), Amazon,, Amazon Fraud AWS Fault Injection Service Detector, Amazon, Server Amazon, Layanan Lokasi EventBridge Amazon,, Amazon Lex FSx, Amazon Lightsail, GameLift Amazon Pinpoint, ,,, Amazon, Basis Data Relasional Amazon AWS IoT OpsWorks AWS Panorama AWS Resource Access Manager QuickSight Layanan (Amazon RDS), Amazon AWS RoboMaker Rekognition,,, Amazon Route 53 AWS Resource Groups, Amazon Simple Storage Service AWS Cloud Map(Amazon S3),, dan. AWS Security Token Service	Oktober 19, 2022

Perubahan	Deskripsi	Tanggal
databrew:ListRecipeVersions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsite		

Perubahan	Deskripsi	Tanggal
wise:DescribePortal, iotsitewise:DescribeProject, iotsitewise:ListAssetModels, iotsitewise:ListDashboards, iotsitewise:ListGateways, iotsitewise:ListPortals, iotsitewise:ListProjectAssets, iotsitewise:ListProjects, iotsitewise:ListTagsForResource, iotwireless:GetServiceProfile, iotwireless:GetWirelessDevice, iotwireless:GetWirelessGatewayTaskDefinition, iotwireless:ListServiceProfiles, iotwireless:ListTagsForResource, iotwireless:ListWirelessDevices, iotwireless:ListWirelessGatewayTaskDefinitions, lex:DescribeBotVersion, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDatabase, lightsail:GetRelationalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign, mobiletargeting:GetSegment, mobiletargeting:GetSegments, opsworks:DescribeInstances, opsworks:DescribeTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplicationInstance, panorama:Describe		

Perubahan	Deskripsi	Tanggal
ApplicationInstanceDetails, panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes,	Kebijakan ini sekarang mendukung izin tambahan untuk AWS Certificate Manager, Alur Kerja Terkelola Amazon untuk Apache Airflow,,, AWS Amplify Amazon Keyspaces, AWS AppConfig Amazon, Amazon Connect,, CloudWatch Amazon Elastic Compute Cloud (Amazon) AWS Glue DataBrew, Amazon EC2 Elastic Kubernetes Service (Amazon EKS), Amazon,, Amazon Fraud AWS Fault Injection Service Detector, Amazon, Server Amazon, Layanan Lokasi EventBridge Amazon,, Amazon Lex FSx, Amazon Lightsail, GameLift Amazon Pinpoint, ,,, Amazon, Basis Data Relasional Amazon AWS IoT OpsWorks AWS Panorama AWS Resource Access Manager QuickSight Layanan (Amazon RDS), Amazon AWS RoboMaker Rekognition,,, Amazon Route 53 AWS Resource Groups, Amazon Simple Storage Service AWS Cloud Map(Amazon S3),, dan. AWS Security Token Service	Oktober 19, 2022

Perubahan	Deskripsi	Tanggal
databrew:ListRecipeVersions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsite		

Perubahan	Deskripsi	Tanggal
wise:DescribePortal, iotsitewise:DescribeProject, iotsitewise:ListAssetModels, iotsitewise:ListDashboards, iotsitewise:ListGateways, iotsitewise:ListPortals, iotsitewise:ListProjectAssets, iotsitewise:ListProjects, iotsitewise:ListTagsForResource, iotwireless:GetServiceProfile, iotwireless:GetWirelessDevice, iotwireless:GetWirelessGatewayTaskDefinition, iotwireless:ListServiceProfiles, iotwireless:ListTagsForResource, iotwireless:ListWirelessDevices, iotwireless:ListWirelessGatewayTaskDefinitions, lex:DescribeBotVersion, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDatabase, lightsail:GetRelationalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign, mobiletargeting:GetSegment, mobiletargeting:GetSegments, opsworks:DescribeInstances, opsworks:DescribeTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplicationInstance, panorama:Describe		

Perubahan	Deskripsi	Tanggal
ApplicationInstanceDetails, panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan Glue::GetTable	Kebijakan ini sekarang memberikan izin untuk mengambil definisi AWS Glue Tabel dalam Katalog Data untuk tabel tertentu.	14 September 2022
AWS_ConfigRole— Tambahkan Glue::GetTable	Kebijakan ini sekarang memberikan izin untuk mengambil definisi AWS Glue Tabel dalam Katalog Data untuk tabel tertentu.	14 September 2022

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2	Kebijakan ini sekarang mendukung izin tambahan untuk Amazon AppFlow, Amazon, Amazon CloudWatch RUM CloudWatch, Amazon CloudWatch Synthetics, Profil Pelanggan Amazon Connect, ID Suara Amazon Connect, Amazon Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon, EventBridge Skema Amazon,, Detektor Fraud Amazon, Layanan Detektor Penipuan Amazon EventBridge, Server Amazon FinSpace Amazon, Video Interaktif Amazon (Amazon IVS) GameLift , Layanan Dikelola Amazon untuk Apache Flink, Image Builder, Amazon Lex, Amazon Lightsail , DevOps EC2 Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble Pinpoint, Amazon, StudioAmazon Amazon, Pengontrol Pemulihan Aplikasi QuickSight Amazon (Amazon Route 53	7 September 2022

Perubahan	Deskripsi	Tanggal
:DescribeTrafficMirrorFilters, ec2:DescribeTrafficMirrorTargets, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamel	Resolver ARC),, Layanan Penyimpanan Sederhana Amazon (Amazon S3) Simple Storage S3), Amazon SimpleDB, Layanan Email Sederhana Amazon (Amazon SES), Amazon Timestream,,,,,,,,,,,,,,,, AWS AppConfig AWS AppSync AWS Auto Scaling AWS Backup AWS Budgets AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise, AWS IoT TwinMaker, AWS Lake Formation, AWS License Manager, AWS Resilience Hub, AWS Signer, dan AWS Transfer Family.	

Perubahan	Deskripsi	Tanggal
ift:DescribeFleetCapacity, gamelift:DescribeFleetLocationAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimensio		

Perubahan	Deskripsi	Tanggal
n, iot:DescribeRoleAlias, iot:DescribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset,		

Perubahan	Deskripsi	Tanggal
iotsitewise:ListAccessPolic ies, iotsitewise:ListAssets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail		

Perubahan	Deskripsi	Tanggal
:GetAlarms, lightsail:GetBuckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsFo		

Perubahan	Deskripsi	Tanggal
rResource, mobiletargeting: GetInAppTemplate, mobiletar geting:ListTemplates, mq:De scribeBroker, mq:ListBr okers, nimble:GetLaunchPr ofile, nimble:GetLaunchProf ileDetails, nimble:GetStreamin gImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponent s, nimble:ListStudios, profile :GetDomain, profile:GetIntegra tion, profile:GetProfileObj ectType, profile:ListDomain s, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis , quicksight:DescribeAnalys isPermissions, quicksight:D escribeDataSet, quicksight: DescribeDataSetPermissions, quicksight:DescribeTheme, q uicksight:DescribeThemePerm issions, quicksight:ListAna lyses, quicksight:ListDataS ets, quicksight:ListThemes, resiliencehub:Describe App, resiliencehub:Describe AppVersionTemplate, resilie ncehub:DescribeResiliencyPo licy, resiliencehub:ListApps, resiliencehub:ListApp		

Perubahan	Deskripsi	Tanggal
VersionResourceMappings, resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-		

Perubahan	Deskripsi	Tanggal
outposts:GetAccessPoint, s3-outposts:GetAccessPoint Policy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetLifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, time		

Perubahan	Deskripsi	Tanggal
stream:ListTagsForResource, transfer:DescribeServer, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan appconfig :ListApplications, appflow: DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:Descri beScalingPlanResources, autoscaling-plans:Des cribeScalingPlans, autoscal ing-plans:GetScalingPlanRes ourceForecastData, autoscal ing:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetActio n, budgets:DescribeBudgetAc tionsForAccount, budgets:De scribeBudgetActionsForBudge t, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironment Memberships, cloud9:Describ eEnvironments, cloud9:Li stEnvironments, cloud9:List TagsForResource, cloudwatc h:GetMetricStream, cloudwat ch:ListMetricStreams, datasync:DescribeLocati onFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2	Kebijakan ini sekarang mendukung izin tambahan untuk Amazon AppFlow, Amazon, Amazon CloudWatc h RUM CloudWatch, Amazon CloudWatch Synthetics, Profil Pelanggan Amazon Connect, ID Suara Amazon Connect, Amazon Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon, EventBridge Skema Amazon,, Detektor Fraud Amazon, Layanan Detektor Penipuan Amazon EventBrid ge, Server Amazon FinSpace Amazon, Video Interakti f Amazon (Amazon IVS) GameLift , Layanan Dikelola Amazon untuk Apache Flink, Image Builder, Amazon Lex, Amazon Lightsail , DevOps EC2 Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble Pinpoint, Amazon, StudioAma zon Amazon, Pengontrol Pemulihan Aplikasi QuickSigh t Amazon (Amazon Route 53	7 September 2022

Perubahan	Deskripsi	Tanggal
:DescribeTrafficMirrorTargets, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity,	Resolver ARC),, Layanan Penyimpanan Sederhana Amazon (Amazon S3) Simple Storage S3), Amazon SimpleDB, Layanan Email Sederhana Amazon (Amazon SES), Amazon Timestream,,,,,,,,,,,,,,,, AWS AppConfig AWS AppSync AWS Auto Scaling AWS Backup AWS Budgets AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise, AWS IoT TwinMaker, AWS Lake Formation, AWS License Manager, AWS Resilience Hub, AWS Signer, dan AWS Transfer Family	

Perubahan	Deskripsi	Tanggal
gamelift:DescribeFleetLocationAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias,		

Perubahan	Deskripsi	Tanggal
iot:DescribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolic		

Perubahan	Deskripsi	Tanggal
ies, iotsitewise:ListAssets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu		

Perubahan	Deskripsi	Tanggal
ckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:		

Perubahan	Deskripsi	Tanggal
GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings,		

Perubahan	Deskripsi	Tanggal
resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint,		

Perubahan	Deskripsi	Tanggal
s3-outposts:GetAccessPoint Policy, s3-outposts:GetBuc ket, s3-outposts:GetBucketP olicy, s3-outposts:GetBuc ketTagging, s3-outposts:Get LifecycleConfiguration, s3- outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuc kets, schemas:DescribeDi scoverer, schemas:DescribeR egistry, schemas:DescribeSc hema, schemas:ListDiscovere rs, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListD omains, ses:ListEmailTempla tes, ses:ListReceiptFilters, ses:ListReceiptRuleSe ts, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissio ns, signer:ListSigningProfiles, synthetics:DescribeCanaries , synthetics:DescribeCanari esLastRun, synthetics:Descr ibeRuntimeVersions, synthetic s:GetCanary, synthetics:Get CanaryRuns, synthetic s:ListTagsForResource, time stream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, time stream:ListTagsForResource,		

Perubahan	Deskripsi	Tanggal
transfer:DescribeServer, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject,	Kebijakan ini sekarang mendukung izin tambahan untuk Alur Kerja Terkelola Amazon untuk Apache Airflow, AWS IoT Amazon 2.0, Amazon CodeGuru Reviewer AppStream ,, Amazon Kinesis AWS HealthLake Video Streams, Amazon Application Recovery Controller (ARC), Amazon Elastic Compute Cloud (AWS Device Farm Amazon), Amazon Pinpoint, (IAM EC2), Amazon AWS Identity and Access Management , dan Log Amazon. GuardDuty CloudWatch	1 Februari 2023

Perubahan	Deskripsi	Tanggal
devicefarm:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar	Kebijakan ini sekarang mendukung izin tambahan untuk Alur Kerja Terkelola Amazon untuk Apache Airflow, AWS IoT Amazon 2.0, Amazon CodeGuru Reviewer AppStream ,, Amazon Kinesis AWS HealthLake Video Streams, Amazon Application Recovery Controller (ARC), Amazon Elastic Compute Cloud (AWS Device Farm Amazon), Amazon Pinpoint, (IAM EC2), Amazon AWS Identity and Access Management , dan Log Amazon. GuardDuty CloudWatch	1 Februari 2023

Perubahan	Deskripsi	Tanggal
m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		
ConfigConformsServiceRolePolicy— Perbarui config:DescribeConfigRules	Sebagai praktik terbaik keamanan, kebijakan ini sekarang menghapus izin tingkat sumber daya yang luas untuk. `config:DescribeConfigRules`	Januari 12, 2023

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, AWS Transfer Family devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager	Kebijakan ini sekarang mendukung izin tambahan untuk Amazon Managed Service untuk Prometheus AWS Audit Manager,,, (), AWS Device Farm Amazon Elastic Compute Cloud AWS Database Migration Service (Amazon AWS DMS), AWS Directory Service,, Amazon AWS IoT Lightsail,,, Amazon EC2, AWS Glue, Amazon Application Recovery Controller (ARC) AWS Elemental MediaPackage QuickSight, AWS Network Manager Amazon Simple Storage Service (AWS Resource Access Manager Amazon S3), dan Amazon Timestream.	Desember 15, 2022

Perubahan	Deskripsi	Tanggal
:GetTransitGatewayRegistrations, networkmanager:ListTagsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTa	Kebijakan ini sekarang mendukung izin tambahan untuk Amazon Managed Service untuk Prometheus AWS Audit Manager,,, (), AWS Device Farm Amazon Elastic Compute Cloud AWS Database Migration Service (Amazon AWS DMS), AWS Directory Service,, Amazon AWS IoT Lightsail,,, Amazon EC2, AWS Glue, Amazon Application Recovery Controller (ARC) AWS Elemental MediaPackage QuickSight, AWS Network Manager Amazon Simple Storage Service (AWS Resource Access Manager Amazon S3), dan Amazon Timestream.	15 Desember 2022

Perubahan	Deskripsi	Tanggal
gsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan cloudformation:ListStackResources and cloudformation:ListStacks	Kebijakan ini sekarang memberikan izin untuk menampilkan deskripsi semua sumber daya dari AWS CloudFormation tumpukan tertentu dan mengembalikan informasi ringkasan untuk tumpukan yang statusnya cocok dengan yang ditentukan. StackStatusFilter	7 November 2022
AWS_ConfigRole— Tambahkan cloudformation:ListStackResources and cloudformation:ListStacks	Kebijakan ini sekarang memberikan izin untuk menampilkan deskripsi semua sumber daya dari AWS CloudFormation tumpukan tertentu dan mengembalikan informasi ringkasan untuk tumpukan yang statusnya cocok dengan yang ditentukan. StackStatusFilter	7 November 2022

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes,	Kebijakan ini sekarang mendukung izin tambahan untuk AWS Certificate Manager, Alur Kerja Terkelola Amazon untuk Apache Airflow,,, AWS Amplify Amazon Keyspaces, AWS AppConfig Amazon, Amazon Connect,, CloudWatch Amazon Elastic Compute Cloud (Amazon) AWS Glue DataBrew, Amazon EC2 Elastic Kubernetes Service (Amazon EKS), Amazon,, Amazon Fraud AWS Fault Injection Service Detector, Amazon, Server Amazon, Layanan Lokasi EventBridge Amazon,, Amazon Lex FSx, Amazon Lightsail, GameLift Amazon Pinpoint, ,,, Amazon, Basis Data Relasional Amazon AWS IoT OpsWorks AWS Panorama AWS Resource Access Manager QuickSight Layanan (Amazon RDS), Amazon AWS RoboMaker Rekognition,,, Amazon Route 53 AWS Resource Groups, Amazon Simple Storage Service AWS Cloud Map(Amazon S3),, dan. AWS Security Token Service	Oktober 19, 2022

Perubahan	Deskripsi	Tanggal
databrew:ListRecipeVersions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsite		

Perubahan	Deskripsi	Tanggal
wise:DescribePortal, iotsitewise:DescribeProject, iotsitewise:ListAssetModels, iotsitewise:ListDashboards, iotsitewise:ListGateways, iotsitewise:ListPortals, iotsitewise:ListProjectAssets, iotsitewise:ListProjects, iotsitewise:ListTagsForResource, iotwireless:GetServiceProfile, iotwireless:GetWirelessDevice, iotwireless:GetWirelessGatewayTaskDefinition, iotwireless:ListServiceProfiles, iotwireless:ListTagsForResource, iotwireless:ListWirelessDevices, iotwireless:ListWirelessGatewayTaskDefinitions, lex:DescribeBotVersion, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDatabase, lightsail:GetRelationalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign, mobiletargeting:GetSegment, mobiletargeting:GetSegments, opsworks:DescribeInstances, opsworks:DescribeTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplicationInstance, panorama:Describe		

Perubahan	Deskripsi	Tanggal
ApplicationInstanceDetails, panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes,	Kebijakan ini sekarang mendukung izin tambahan untuk AWS Certificate Manager, Alur Kerja Terkelola Amazon untuk Apache Airflow,,, AWS Amplify Amazon Keyspaces, AWS AppConfig Amazon, Amazon Connect,, CloudWatch Amazon Elastic Compute Cloud (Amazon) AWS Glue DataBrew, Amazon EC2 Elastic Kubernetes Service (Amazon EKS), Amazon,, Amazon Fraud AWS Fault Injection Service Detector, Amazon, Server Amazon, Layanan Lokasi EventBridge Amazon,, Amazon Lex FSx, Amazon Lightsail, GameLift Amazon Pinpoint, ,,, Amazon, Basis Data Relasional Amazon AWS IoT OpsWorks AWS Panorama AWS Resource Access Manager QuickSight Layanan (Amazon RDS), Amazon AWS RoboMaker Rekognition,,, Amazon Route 53 AWS Resource Groups, Amazon Simple Storage Service AWS Cloud Map(Amazon S3),, dan. AWS Security Token Service	Oktober 19, 2022

Perubahan	Deskripsi	Tanggal
databrew:ListRecipeVersions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsite		

Perubahan	Deskripsi	Tanggal
wise:DescribePortal, iotsitewise:DescribeProject, iotsitewise:ListAssetModels, iotsitewise:ListDashboards, iotsitewise:ListGateways, iotsitewise:ListPortals, iotsitewise:ListProjectAssets, iotsitewise:ListProjects, iotsitewise:ListTagsForResource, iotwireless:GetServiceProfile, iotwireless:GetWirelessDevice, iotwireless:GetWirelessGatewayTaskDefinition, iotwireless:ListServiceProfiles, iotwireless:ListTagsForResource, iotwireless:ListWirelessDevices, iotwireless:ListWirelessGatewayTaskDefinitions, lex:DescribeBotVersion, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDatabase, lightsail:GetRelationalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign, mobiletargeting:GetSegment, mobiletargeting:GetSegments, opsworks:DescribeInstances, opsworks:DescribeTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplicationInstance, panorama:Describe		

Perubahan	Deskripsi	Tanggal
ApplicationInstanceDetails, panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan Glue::GetTable	Kebijakan ini sekarang memberikan izin untuk mengambil definisi AWS Glue Tabel dalam Katalog Data untuk tabel tertentu.	14 September 2022
AWS_ConfigRole— Tambahkan Glue::GetTable	Kebijakan ini sekarang memberikan izin untuk mengambil definisi AWS Glue Tabel dalam Katalog Data untuk tabel tertentu.	14 September 2022

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2	Kebijakan ini sekarang mendukung izin tambahan untuk Amazon AppFlow, Amazon, Amazon CloudWatch RUM CloudWatch, Amazon CloudWatch Synthetics, Profil Pelanggan Amazon Connect, ID Suara Amazon Connect, Amazon Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon, EventBridge Skema Amazon,, Detektor Fraud Amazon, Layanan Detektor Penipuan Amazon EventBridge, Server Amazon FinSpace Amazon, Video Interaktif Amazon (Amazon IVS) GameLift , Layanan Dikelola Amazon untuk Apache Flink, Image Builder, Amazon Lex, Amazon Lightsail , DevOps EC2 Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble Pinpoint, Amazon, StudioAmazon Amazon, Pengontrol Pemulihan Aplikasi QuickSight Amazon (Amazon Route 53	7 September 2022

Perubahan	Deskripsi	Tanggal
:DescribeTrafficMirrorFilters, ec2:DescribeTrafficMirrorTargets, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamel	Resolver ARC),, Layanan Penyimpanan Sederhana Amazon (Amazon S3) Simple Storage S3), Amazon SimpleDB, Layanan Email Sederhana Amazon (Amazon SES), Amazon Timestream,,,,,,,,,,,,,,,, AWS AppConfig AWS AppSync AWS Auto Scaling AWS Backup AWS Budgets AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise, AWS IoT TwinMaker, AWS Lake Formation, AWS License Manager, AWS Resilience Hub, AWS Signer, dan AWS Transfer Family.	

Perubahan	Deskripsi	Tanggal
ift:DescribeFleetCapacity, gamelift:DescribeFleetLocationAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimensio		

Perubahan	Deskripsi	Tanggal
n, iot:DescribeRoleAlias, iot:DescribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset,		

Perubahan	Deskripsi	Tanggal
iotsitewise:ListAccessPolic ies, iotsitewise:ListAssets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail		

Perubahan	Deskripsi	Tanggal
:GetAlarms, lightsail:GetBuckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsFo		

Perubahan	Deskripsi	Tanggal
rResource, mobiletargeting: GetInAppTemplate, mobiletar geting:ListTemplates, mq:De scribeBroker, mq:ListBr okers, nimble:GetLaunchPr ofile, nimble:GetLaunchProf ileDetails, nimble:GetStreamin gImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponent s, nimble:ListStudios, profile :GetDomain, profile:GetIntegra tion, profile:GetProfileObj ectType, profile:ListDomain s, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis , quicksight:DescribeAnalys isPermissions, quicksight:D escribeDataSet, quicksight: DescribeDataSetPermissions, quicksight:DescribeTheme, q uicksight:DescribeThemePerm issions, quicksight:ListAna lyses, quicksight:ListDataS ets, quicksight:ListThemes, resiliencehub:Describe App, resiliencehub:Describe AppVersionTemplate, resilie ncehub:DescribeResiliencyPo licy, resiliencehub:ListApps, resiliencehub:ListApp		

Perubahan	Deskripsi	Tanggal
VersionResourceMappings, resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-		

Perubahan	Deskripsi	Tanggal
outposts:GetAccessPoint, s3-outposts:GetAccessPoint Policy, s3-outposts:GetBuc ket, s3-outposts:GetBucketP olicy, s3-outposts:GetBuc ketTagging, s3-outposts:Get LifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuc kets, schemas:DescribeDi scoverer, schemas:DescribeR egistry, schemas:DescribeSc hema, schemas:ListDiscovere rs, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListD omains, ses:ListEmailTempla tes, ses:ListReceiptFilters, ses:ListReceiptRuleSe ts, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissio ns, signer:ListSigningProfiles, synthetics:DescribeCanaries , synthetics:DescribeCanari esLastRun, synthetics:Descr ibeRuntimeVersions, synthetic s:GetCanary, synthetics:Get CanaryRuns, synthetic s:ListTagsForResource, time stream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, time		

Perubahan	Deskripsi	Tanggal
stream:ListTagsForResource, transfer:DescribeServer, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan appconfig :ListApplications, appflow: DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:Descri beScalingPlanResources, autoscaling-plans:Des cribeScalingPlans, autoscal ing-plans:GetScalingPlanRes ourceForecastData, autoscal ing:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetActio n, budgets:DescribeBudgetAc tionsForAccount, budgets:De scribeBudgetActionsForBudge t, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironment Memberships, cloud9:Describ eEnvironments, cloud9:Li stEnvironments, cloud9:List TagsForResource, cloudwatc h:GetMetricStream, cloudwat ch:ListMetricStreams, datasync:DescribeLocati onFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2	Kebijakan ini sekarang mendukung izin tambahan untuk Amazon AppFlow, Amazon, Amazon CloudWatc h RUM CloudWatch, Amazon CloudWatch Synthetics, Profil Pelanggan Amazon Connect, ID Suara Amazon Connect, Amazon Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon, EventBridge Skema Amazon,, Detektor Fraud Amazon, Layanan Detektor Penipuan Amazon EventBrid ge, Server Amazon FinSpace Amazon, Video Interakti f Amazon (Amazon IVS) GameLift , Layanan Dikelola Amazon untuk Apache Flink, Image Builder, Amazon Lex, Amazon Lightsail , DevOps EC2 Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble Pinpoint, Amazon, StudioAma zon Amazon, Pengontrol Pemulihan Aplikasi QuickSigh t Amazon (Amazon Route 53	7 September 2022

Perubahan	Deskripsi	Tanggal
:DescribeTrafficMirrorTargets, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity,	Resolver ARC),, Layanan Penyimpanan Sederhana Amazon (Amazon S3) Simple Storage S3), Amazon SimpleDB, Layanan Email Sederhana Amazon (Amazon SES), Amazon Timestream,,,,,,,,,,,,,,,, AWS AppConfig AWS AppSync AWS Auto Scaling AWS Backup AWS Budgets AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise, AWS IoT TwinMaker, AWS Lake Formation, AWS License Manager, AWS Resilience Hub, AWS Signer, dan AWS Transfer Family	

Perubahan	Deskripsi	Tanggal
gamelift:DescribeFleetLocationAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias,		

Perubahan	Deskripsi	Tanggal
iot:DescribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolic		

Perubahan	Deskripsi	Tanggal
ies, iotsitewise:ListAssets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu		

Perubahan	Deskripsi	Tanggal
ckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:		

Perubahan	Deskripsi	Tanggal
GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings,		

Perubahan	Deskripsi	Tanggal
resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint,		

Perubahan	Deskripsi	Tanggal
s3-outposts:GetAccessPoint Policy, s3-outposts:GetBuc ket, s3-outposts:GetBucketP olicy, s3-outposts:GetBuc ketTagging, s3-outposts:Get LifecycleConfiguration, s3- outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuc kets, schemas:DescribeDi scoverer, schemas:DescribeR egistry, schemas:DescribeSc hema, schemas:ListDiscovere rs, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListD omains, ses:ListEmailTempla tes, ses:ListReceiptFilters, ses:ListReceiptRuleSe ts, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissio ns, signer:ListSigningProfiles, synthetics:DescribeCanaries , synthetics:DescribeCanari esLastRun, synthetics:Descr ibeRuntimeVersions, synthetic s:GetCanary, synthetics:Get CanaryRuns, synthetic s:ListTagsForResource, time stream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, time stream:ListTagsForResource,		

Perubahan	Deskripsi	Tanggal
transfer:DescribeServer, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		
AWSConfigServiceRolePolicy— Tambahkan datasync:ListAgents, datasync:ListLocations, datasync:ListTasks, servicediscovery:ListNamespaces, servicediscovery:ListServices, and ses:ListContactLists	Kebijakan ini sekarang memberikan izin untuk menampilkan daftar AWS DataSync agen, lokasi DataSync sumber dan tujuan, serta DataSync tugas dalam Akun AWS; daftar informasi ringkasan tentang AWS Cloud Map ruang nama dan layanan yang terkait dengan satu atau beberapa ruang nama tertentu dalam Akun AWS; dan daftar semua daftar kontak Amazon Simple Email Service (Amazon SES) yang tersedia di. Akun AWS	22 Agustus 2022

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan datasync: ListAgents, datasync:ListLocations, datasync:ListTasks, servicediscovery:ListNamespaces, servicediscovery:ListServices, and ses:ListContactLists	Kebijakan ini sekarang memberikan izin untuk menampilkan daftar AWS DataSync agen, lokasi DataSync sumber dan tujuan, serta DataSync tugas dalam Akun AWS; daftar informasi ringkasan tentang AWS Cloud Map ruang nama dan layanan yang terkait dengan satu atau beberapa ruang nama tertentu dalam Akun AWS; dan daftar semua daftar kontak Amazon Simple Email Service (Amazon SES) yang tersedia di. Akun AWS	22 Agustus 2022
ConfigConformsServiceRolePolicy— Tambahkan cloudwatch:PutMetricData	Kebijakan ini sekarang memberikan izin untuk mempublikasikan titik data metrik ke Amazon CloudWatch.	25 Juli 2022

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan amplifyuibuilder:ExportThemes, amplifyuibuilder:GetTheme, appconfig:GetApplication, appconfig:GetApplication, appconfig:GetConfigurationProfile, appconfig:GetConfigurationProfile, appconfig:GetDeployment, appconfig:GetDeploymentStrategy, appconfig:GetEnvironment, appconfig:GetHostedConfigurationVersion, appconfig:ListTagsForResource, appsync:GetGraphqlApi, appsync:ListGraphqlApis, billingconductor: ListPricingRulesAssociatedToPricingPlan, billingconductor:ListAccountAssociations, billingconductor:ListBillingGroups, billingconductor:ListCustomLineItems, billingconductor:ListPricingPlans, billingconductor:ListPricingRules, billingconductor:ListTagsForResource, datasync:DescribeAgent, datasync:DescribeLocationEfs, datasync:DescribeLocationFsxLustre, datasync:DescribeLocationHdfs, datasync:DescribeLocationNfs, datasync:DescribeLocatio	Kebijakan ini sekarang mendukung izin tambahan untuk Amazon Elastic Container Service (Amazon ECS), Amazon, Amazon, Amazon, Amazon, ElastiCache Amazon Managed Service untuk Apache Flink FSx, EventBridge Amazon Location Service, Amazon Managed Streaming untuk Apache Kafka Kafka, Amazon, Amazon Rekognition,, Amazon QuickSight Simple Storage Service (Amazon S3) Storage Service S3) AWS RoboMaker, Amazon Simple Email Service (Amazon SES),,,,,,, (Pusat Identitas IAM AWS Amplify) AWS AppConfig, Image Builder AWS Firewall Manager, AWS Glue dan AWS Billing Conductor AWS DataSync Beban AWS AppSync Elastis AWS IAM Identity Center EC2 Menyeimbangkan.	15 Juli 2022

Perubahan	Deskripsi	Tanggal
nObjectStorage, datasync:DescribeLocationS3, datasync:DescribeLocationSmb, datasync:DescribeTask, datasync:ListTagsForResource, ecr:DescribePullThroughCacheRules, ecr:DescribeRegistry, ecr:GetRegistryPolicy, elasticache:DescribeCacheParameters, elasticloadbalancing:DescribeListenerCertificates, elasticloadbalancing:DescribeTargetGroupAttributes, elasticloadbalancing:DescribeTargetGroups, elasticloadbalancing:DescribeTargetHealth, events:DescribeApiDestination, events:DescribeArchive, fms:GetNotificationChannel, fms:GetPolicy, fms:ListPolicies, fms:ListTagsForResource, fsx:DescribeVolumes, geo:DescribeGeofenceCollection, geo:DescribeMap, geo:DescribePlaceIndex, geo:DescribeRouteCalculator, geo:DescribeTracker, geo:ListTrackerConsumers, glue:BatchGetJobs, glue:BatchGetWorkflows, glue:GetCrawler, glue:GetCrawlers, glue:GetJob, glue:GetJobs, glue:GetWorkflow, imagebuilder: GetComponent, imagebuilder: ListComponentBuildVers		

Perubahan	Deskripsi	Tanggal
ions, imagebuilder: ListCompo nents, imagebuilder:GetDist ributionConfiguration, imag ebuilder:GetInfrastructureC onfiguration, imagebuilder: ListDistributionConfigurati ons, imagebuilder:ListInfra structureConfigurations, kafka:DescribeClusterV2, kafka:ListClustersV2, kines isanalytics:DescribeApplica tion, kinesisanalytics:List TagsForResource, quicksight :DescribeDataSource, quicksight:DescribeDataS ourcePermissions, quicksigh t:ListTagsForResource, reko gnition:DescribeStreamProce ssor, rekognition:ListTagsF orResource, robomaker:Descr ibeRobotApplication, roboma ker:DescribeSimulationAppli cation, s3:GetStorageLensCo nfiguration, s3:GetStorageL ensConfigurationTagging, se rvicediscovery:GetInstance, servicediscovery:GetNamespa ce, servicediscovery:GetSer vice, servicediscovery:List TagsForResource, ses:Descr ibeReceiptRule, ses:Describ eReceiptRuleSet, ses:GetCo ntactList, ses:GetEmailTemp late, ses:GetTemplate, and		

Perubahan	Deskripsi	Tanggal
sso:GetInlinePolicyForPermissionSet		

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan amplifyuibuilder:ExportThemes, amplifyuibuilder:GetTheme, appconfig:GetApplication, appconfig:GetApplication, appconfig:GetConfigurationProfile, appconfig:GetConfigurationProfile, appconfig:GetDeployment, appconfig:GetDeploymentStrategy, appconfig:GetEnvironment, appconfig:GetHostedConfigurationVersion, appconfig:ListTagsForResource, appsync:GetGraphqlApi, appsync:ListGraphqlApis, billingconductor:ListPricingRulesAssociatedToPricingPlan, billingconductor:ListAccountAssociations, billingconductor:ListBillingGroups, billingconductor:ListCustomLineItems, billingconductor:ListPricingPlans, billingconductor:ListPricingRules, billingconductor:ListTagsForResource, datasync:DescribeAgent, datasync:DescribeLocationEfs, datasync:DescribeLocationFsxLustre, datasync:DescribeLocationHdfs, datasync:DescribeLocationNfs, datasync:DescribeLocatio	Kebijakan ini sekarang mendukung izin tambahan untuk Amazon Elastic Container Service (Amazon ECS), Amazon, Amazon, Amazon, Amazon, ElastiCache Amazon Managed Service untuk Apache Flink FSx, EventBridge Amazon Location Service, Amazon Managed Streaming untuk Apache Kafka Kafka, Amazon, Amazon Rekognition,, Amazon QuickSight Simple Storage Service (Amazon S3) Storage Service S3) AWS RoboMaker, Amazon Simple Email Service (Amazon SES),,,,,,, (Pusat Identitas IAM AWS Amplify) AWS AppConfig, Image Builder AWS Firewall Manager, AWS Glue dan AWS Billing Conductor AWS DataSync Beban AWS AppSync Elastis AWS IAM Identity Center EC2 Menyeimbangkan.	15 Juli 2022

Perubahan	Deskripsi	Tanggal
nObjectStorage, datasync:DescribeLocationS3, datasync:DescribeLocationSmb, datasync:DescribeTask, datasync:ListTagsForResource, ecr:DescribePullThroughCacheRules, ecr:DescribeRegistry, ecr:GetRegistryPolicy, elasticache:DescribeCacheParameters, elasticloadbalancing:DescribeListenerCertificates, elasticloadbalancing:DescribeTargetGroupAttributes, elasticloadbalancing:DescribeTargetGroups, elasticloadbalancing:DescribeTargetHealth, events:DescribeApiDestination, events:DescribeArchive, fms:GetNotificationChannel, fms:GetPolicy, fms:ListPolicies, fms:ListTagsForResource, fsx:DescribeVolumes, geo:DescribeGeofenceCollection, geo:DescribeMap, geo:DescribePlaceIndex, geo:DescribeRouteCalculator, geo:DescribeTracker, geo:ListTrackerConsumers, glue:BatchGetJobs, glue:BatchGetWorkflows, glue:GetCrawler, glue:GetCrawlers, glue:GetJob, glue:GetJobs, glue:GetWorkflow, imagebuilder: GetComponent, imagebuilder: ListComponentBuildVers		

Perubahan	Deskripsi	Tanggal
ions, imagebuilder: ListComponents, imagebuilder:GetDistributionConfiguration, imagebuilder:GetInfrastructureConfiguration, imagebuilder:ListDistributionConfigurations, imagebuilder:ListInfrastructureConfigurations, kafka:DescribeClusterV2, kafka:ListClustersV2, kinesisanalytics:DescribeApplication, kinesisanalytics:ListTagsForResource, quicksight:DescribeDataSource, quicksight:DescribeDataSourcePermissions, quicksight:ListTagsForResource, rekognition:DescribeStreamProcessor, rekognition:ListTagsForResource, robomaker:DescribeRobotApplication, robomaker:DescribeSimulationApplication, s3:GetStorageLensConfiguration, s3:GetStorageLensConfigurationTagging, servicediscovery:GetInstance, servicediscovery:GetNamespace, servicediscovery:GetService, servicediscovery:ListTagsForResource, ses:DescribeReceiptRule, ses:DescribeReceiptRuleSet, ses:GetContactList, ses:GetEmailTemplate, ses:GetTemplate, and		

Perubahan	Deskripsi	Tanggal
sso:GetInlinePolicyForPermissionSet		

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan athena:GetDataCatalog, athena:ListDataCatalogs, athena:ListTagsForResource, detective:ListGraphs, detective:ListTagsForResource, glue:BatchGetDevEndpoints, glue:GetDevEndpoint, glue:GetDevEndpoints, glue:GetSecurityConfiguration, glue:GetSecurityConfigurations, glue:GetTags glue:GetWorkGroup, glue:ListCrawlers, glue:ListDevEndpoints, glue:ListJobs, glue:ListMembers, glue:ListWorkflows, glue:ListWorkGroups, guardduty:GetFilter, guardduty:GetIPSet, guardduty:GetThreatIntelSet, guardduty:GetMembers, guardduty:ListFilters, guardduty:ListIPSets, guardduty:ListTagsForResource, guardduty:ListThreatIntelSets, macie:GetMacieSession, ram:GetResourceShareAssociations, ram:GetResourceShares, ses:GetConfigurationSet, ses:GetConfigurationSetEventDestinations, ses:ListConfigurationSets, sso:DescribeInstanceAccessControlAtt	Kebijakan ini sekarang memberikan izin untuk mendapatkan katalog data Amazon Athena yang ditentukan, mencantumkan katalog data Athena dalam, dan mencantumkan tag Akun AWS yang terkait dengan grup kerja Athena atau sumber daya katalog data; untuk mendapatkan daftar grafik perilaku Detektif Amazon dan tag daftar untuk grafik perilaku Detektif; dapatkan daftar metadata sumber daya untuk daftar nama titik akhir pengembangan yang diberikan AWS Glue , dapatkan informasi tentang titik akhir pengembangan tertentu, dapatkan semua titik akhir pengembangan di sebuah, ambil keamanan tertentu AWS Glue AWS Glue Akun AWS AWS Glue konfigurasi, dapatkan semua konfigurasi AWS Glue keamanan, dapatkan daftar tag yang terkait dengan AWS Glue sumber daya, dapatkan informasi tentang AWS Glue grup kerja dengan nama yang ditentukan, ambil nama semua sumber	31 Mei 2022

Perubahan	Deskripsi	Tanggal
ributeConfiguration, sso:DescribePermissionSet, sso:ListManagedPoliciesInPermissionSet, sso:ListPermissionSets, and sso:ListTagsForResource	daya AWS Glue crawler di AWS akun, dapatkan nama semua sumber AWS Glue `DevEndpoint` daya dalam, daftar nama semua sumber daya AWS Glue pekerjaan di sebuah Akun AWS, dapatkan detail tentang akun AWS Glue anggota Akun AWS, daftar nama AWS Glue alur kerja yang dibuat di akun, dan daftar grup kerja yang tersedia AWS Glue untuk akun; untuk mengambil detail tentang GuardDuty filter Amazon, mengambil, mengambil GuardDuty IPSet, mengambil akun GuardDuty anggota GuardDutyThreatIntelSet, mendapatkan daftar GuardDuty filter, mendapatkan layanan, mengambil tag untuk Layanan, dan mendapatkan GuardDuty layanan; untuk mendapatkan pengaturan status dan konfigurasi saat ini untuk akun Amazon Macie; untuk mengambil sumber daya dan asosiasi utama untuk AWS Resource Access Manager ()AWS RAM pembagian sumber daya dan mengambil detail tentang sumber daya IPSets GuardDuty ThreatInt	

Perubahan	Deskripsi	Tanggal
	elSets GuardDuty AWS RAM berbagi; untuk mendapatkan informasi tentang set konfigura si Amazon Simple Email Service (Amazon SES) yang ada, dapatkan daftar tujuan acara yang terkait dengan set konfigurasi Amazon SES, dan daftarkan semua set konfigura si yang terkait dengan akun Amazon SES; dan untuk mendapatkan daftar atribut direktori Pusat Identitas, dapatkan detail kumpulan izin, dapatkan kebijakan terkelola IAM AWS IAM Identity Center yang dilampirkan ke IAM yang ditentukan Set izin Pusat Identitas, dapatkan izin yang ditetapkan untuk instans Pusat Identitas IAM, dan dapatkan tag untuk Identitas IAM Sumber daya pusat.	

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan athena:GetDataCatalog, athena:ListDataCatalogs, athena:ListTagsForResource, detective:ListGraphs, detective:ListTagsForResource, glue:BatchGetDevEndpoints, glue:GetDevEndpoint, glue:GetDevEndpoints, glue:GetSecurityConfiguration, glue:GetSecurityConfigurations, glue:GetTags glue:GetWorkGroup, glue:ListCrawlers, glue:ListDevEndpoints, glue:ListJobs, glue:ListMembers, glue:ListWorkflows, glue:ListWorkGroups, guardduty:GetFilter, guardduty:GetIPSet, guardduty:GetThreatIntelSet, guardduty:GetMembers, guardduty:ListFilters, guardduty:ListIPSets, guardduty:ListTagsForResource, guardduty:ListThreatIntelSets, macie:GetMacieSession, ram:GetResourceShareAssociations, ram:GetResourceShares, ses:GetConfigurationSet, ses:GetConfigurationSetEventDestinations, ses:ListConfigurationSets, sso:DescribeInstanceAccessControlAtt	Kebijakan ini sekarang memberikan izin untuk mendapatkan katalog data Amazon Athena yang ditentukan, mencantumkan katalog data Athena dalam, dan mencantumkan tag Akun AWS yang terkait dengan grup kerja Athena atau sumber daya katalog data; untuk mendapatkan daftar grafik perilaku Detektif Amazon dan tag daftar untuk grafik perilaku Detektif; dapatkan daftar metadata sumber daya untuk daftar nama titik akhir pengembangan yang diberikan AWS Glue , dapatkan informasi tentang titik akhir pengembangan tertentu, dapatkan semua titik akhir pengembangan di sebuah, ambil keamanan tertentu AWS Glue AWS Glue Akun AWS AWS Glue konfigurasi, dapatkan semua konfigurasi AWS Glue keamanan, dapatkan daftar tag yang terkait dengan AWS Glue sumber daya, dapatkan informasi tentang AWS Glue grup kerja dengan nama yang ditentukan, ambil nama semua sumber	31 Mei 2022

Perubahan	Deskripsi	Tanggal
ributeConfiguration, sso:DescribePermissionSet, sso:ListManagedPoliciesInPermissionSet, sso:ListPermissionSets, and sso:ListTagsForResource	daya AWS Glue crawler di AWS akun, dapatkan nama semua sumber AWS Glue `DevEndpoint` daya dalam, daftar nama semua sumber daya AWS Glue pekerjaan di sebuah Akun AWS, dapatkan detail tentang akun AWS Glue anggota Akun AWS, daftar nama AWS Glue alur kerja yang dibuat di akun, dan daftar grup kerja yang tersedia AWS Glue untuk akun; untuk mengambil detail tentang GuardDuty filter Amazon, mengambil, mengambil GuardDuty IPSet, mengambil akun GuardDuty anggota GuardDutyThreatIntelSet, mendapatkan daftar GuardDuty filter, mendapatkan layanan, mengambil tag untuk Layanan, dan mendapatkan GuardDuty layanan; untuk mendapatkan pengaturan status dan konfigurasi saat ini untuk akun Amazon Macie; untuk mengambil sumber daya dan asosiasi utama untuk AWS Resource Access Manager ()AWS RAM pembagian sumber daya dan mengambil detail tentang sumber daya IPSets GuardDuty ThreatInt	

Perubahan	Deskripsi	Tanggal
	elSets GuardDuty AWS RAM berbagi; untuk mendapatkan informasi tentang set konfigura si Amazon Simple Email Service (Amazon SES) yang ada, dapatkan daftar tujuan acara yang terkait dengan set konfigurasi Amazon SES, dan daftarkan semua set konfigura si yang terkait dengan akun Amazon SES; dan untuk mendapatkan daftar atribut direktori Pusat Identitas, dapatkan detail kumpulan izin, dapatkan kebijakan terkelola IAM AWS IAM Identity Center yang dilampirkan ke IAM yang ditentukan Set izin Pusat Identitas, dapatkan izin yang ditetapkan untuk instans Pusat Identitas IAM, dan dapatkan tag untuk Identitas IAM Sumber daya pusat.	

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan cloudformation:GetResource, cloudformation:ListResources, cloudtrail:GetEventDataStore, cloudtrail:ListEventDataStores, dax:DescribeParameterGroups, dax:DescribeParameters, dax:DescribeSubnetGroups, DMS:DescribeReplicationTasks, and organizations:ListPolicies	Kebijakan ini sekarang memberikan izin untuk mendapatkan informasi tentang semua atau penyimpanan data AWS CloudTrail peristiwa tertentu (EDS), mendapatkan informasi tentang semua atau AWS CloudFormation sumber daya tertentu, mendapatkan daftar grup parameter DynamoDB Accelerator (DAX) atau grup subnet, mendapatkan informasi AWS Database Migration Service tentang AWS DMS() tugas replikasi untuk akun Anda di wilayah saat ini yang sedang diakses, dan mendapatkan daftar semua kebijakan dalam tipe tertentu. AWS Organizations	7 April 2022

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan cloudformation:GetResource, cloudformation:ListResources, cloudtrail:GetEventDataStore, cloudtrail:ListEventDataStores, dax:DescribeParameterGroups, dax:DescribeParameters, dax:DescribeSubnetGroups, DMS:DescribeReplicationTasks, and organizations:ListPolicies	Kebijakan ini sekarang memberikan izin untuk mendapatkan informasi tentang semua atau penyimpanan data AWS CloudTrail peristiwa tertentu (EDS), mendapatkan informasi tentang semua atau AWS CloudFormation sumber daya tertentu, mendapatkan daftar grup parameter DynamoDB Accelerator (DAX) atau grup subnet, mendapatkan informasi AWS Database Migration Service tentang AWS DMS() tugas replikasi untuk akun Anda di wilayah saat ini yang sedang diakses, dan mendapatkan daftar semua kebijakan dalam tipe tertentu. AWS Organizations	7 April 2022

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan backup-gateway:ListTagsForResource, backup-gateway:ListVirtualMachines, batch:DescribeComputeEnvironments, batch:DescribeJobQueues, batch:ListTagsForResource, dax:ListTags, dms:DescribeCertificates, dynamodb:DescribeGlobalTable, dynamodb:DescribeGlobalTableSettings, ec2:DescribeClientVpnAuthorizationRules, ec2:DescribeClientVpnEndpoints, ec2:DescribeDhcpOptions, ec2:DescribeFleets, ec2:DescribeNetworkAcls, ec2:DescribePlacementGroups, ec2:DescribeSpotFleetRequests, ec2:DescribeVolumeAttribute, ec2:DescribeVolumes, eks:DescribeFargateProfile, eks:ListFargateProfiles, eks:ListTagsForResource, fsx:ListTagsForResource, guardduty:ListOrganizationAdminAccounts, kms:ListAliases, opsworks:DescribeLayers, opsworks:DescribeStacks, opsworks:ListTags, rds:DescribeDBClusterParameterGroups, rds:DescribeDBClusterPara	Kebijakan ini sekarang mendukung izin tambahan untuk AWS Backup,, DynamoDB AWS Batch Accelerator, Amazon DynamoDB AWS Database Migration Service, Amazon Elastic Compute Cloud (Amazon), Amazon Elastic Kubernetes Service, EC2 Amazon, Amazon, Amazon,,, Amazon Relational Database Service, FSx V2, dan GuardDuty Amazon AWS Key Management Service. AWS OpsWorks AWS WAF WorkSpaces	Maret 14, 2022

Perubahan	Deskripsi	Tanggal
meters, states:DescribeActivity, states:ListActivities, wafv2:GetRuleGroup, wafv2:ListRuleGroups, wafv2:ListTagsForResource, workspaces:DescribeConnectionAliases, workspaces:DescribeTags, and workspaces:DescribeWorkspaces		

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan backup-gateway:ListTagsForResource, backup-gateway:ListVirtualMachines, batch:DescribeComputeEnvironments, batch:DescribeJobQueues, batch:ListTagsForResource, dax:ListTags, dms:DescribeCertificates, dynamodb:DescribeGlobalTable, dynamodb:DescribeGlobalTableSettings, ec2:DescribeClientVpnAuthorizationRules, ec2:DescribeClientVpnEndpoints, ec2:DescribeDhcpOptions, ec2:DescribeFleets, ec2:DescribeNetworkAcls, ec2:DescribePlacementGroups, ec2:DescribeSpotFleetRequests, ec2:DescribeVolumeAttribute, ec2:DescribeVolumes, eks:DescribeFargateProfile, eks:ListFargateProfiles, eks:ListTagsForResource, fsx:ListTagsForResource, guardduty:ListOrganizationAdminAccounts, kms:ListAliases, opsworks:DescribeLayers, opsworks:DescribeStacks, opsworks:ListTags, rds:DescribeDBClusterParameterGroups, rds:DescribeDBClusterPara	Kebijakan ini sekarang mendukung izin tambahan untuk AWS Backup,, DynamoDB AWS Batch Accelerator, Amazon DynamoDB AWS Database Migration Service, Amazon Elastic Compute Cloud (Amazon), Amazon Elastic Kubernetes Service, EC2 Amazon, Amazon, Amazon,,, Amazon Relational Database Service, FSx V2, dan GuardDuty Amazon AWS Key Management Service. AWS OpsWorks AWS WAF WorkSpaces	Maret 14, 2022

Perubahan	Deskripsi	Tanggal
meters, states:DescribeActivity, states:ListActivities, wafv2:GetRuleGroup, wafv2:ListRuleGroups, wafv2:ListTagsForResource, workspaces:DescribeConnectionAliases, workspaces:DescribeTags, and workspaces:DescribeWorkspaces		

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan elasticbeanstalk:DescribeEnvironments, elasticbeanstalk:DescribeConfigurationSettings, account:GetAlternateContact, organizations:DescribePolicy, organizations:ListParents, organizations:ListPoliciesForTarget, es:GetCompatibleElasticsearchVersions, rds:DescribeOptionGroups, rds:DescribeOptionGroups, es:GetCompatibleVersions, codedeploy:GetDeploymentConfig, ecr-public:GetRepositoryPolicy, access-analyzer:GetArchiveRule, and ecs:ListTaskDefinitionFamilies	Kebijakan ini sekarang memberikan izin untuk mendapatkan detail tentang lingkungan Elastic Beanstalk dan deskripsi pengaturan untuk set konfigurasi Elastic Beanstalk yang ditentukan, mendapatkan peta atau versi Elasticsearch, menjelaskan grup opsi Amazon OpenSearch RDS yang tersedia untuk database, dan mendapatkan informasi tentang konfigurasi penerapan. CodeDeploy Kebijakan ini juga sekarang memberikan izin untuk mengambil kontak alternatif tertentu yang dilampirkan pada Akun AWS, mengambil informasi tentang kebijakan, mengambil AWS Organizations kebijakan repositori Amazon ECR, mengambil informasi tentang aturan yang AWS Config diarsipkan, mengambil daftar keluarga definisi tugas Amazon ECS, mencantumkan OUs unit organisasi root atau induk () dari OU atau akun turunan yang ditentukan, dan daftar kebijakan yang dilampirkan ke root target, unit organisasi, atau akun yang ditentukan.	Februari 10, 2022

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan elasticbeanstalk:DescribeEnvironments, elasticbeanstalk:DescribeConfigurationSettings, account:GetAlternateContact, organizations:DescribePolicy, organizations:ListParents, organizations:ListPoliciesForTarget, es:GetCompatibleElasticsearchVersions, rds:DescribeOptionGroups, rds:DescribeOptionGroups, es:GetCompatibleVersions, codedeploy:GetDeploymentConfig, ecr-public:GetRepositoryPolicy, access-analyzer:GetArchiveRule, and ecs:ListTaskDefinitionFamilies	Kebijakan ini sekarang memberikan izin untuk mendapatkan detail tentang lingkungan Elastic Beanstalk dan deskripsi pengaturan untuk set konfigurasi Elastic Beanstalk yang ditentukan, mendapatkan peta atau versi Elasticsearch, menjelaskan grup opsi Amazon OpenSearch RDS yang tersedia untuk database, dan mendapatkan informasi tentang konfigurasi penerapan. CodeDeploy Kebijakan ini juga sekarang memberikan izin untuk mengambil kontak alternatif tertentu yang dilampirkan pada Akun AWS, mengambil informasi tentang kebijakan, mengambil AWS Organizations kebijakan repositori Amazon ECR, mengambil informasi tentang aturan yang AWS Config diarsipkan, mengambil daftar keluarga definisi tugas Amazon ECS, mencantumkan OUs unit organisasi root atau induk () dari OU atau akun turunan yang ditentukan, dan daftar kebijakan yang dilampirkan ke root target, unit organisasi, atau akun yang ditentukan.	Februari 10, 2022

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan logs:CreateLogStream, logs:CreateLogGroup, and logs:PutLogEvent	Kebijakan ini sekarang memberikan izin untuk membuat grup dan aliran CloudWatch log Amazon dan menulis log ke aliran log yang dibuat.	Desember 15, 2021
AWS_ConfigRole— Tambahkan logs:CreateLogStream, logs:CreateLogGroup, and logs:PutLogEvent	Kebijakan ini sekarang memberikan izin untuk membuat grup dan aliran CloudWatch log Amazon dan menulis log ke aliran log yang dibuat.	Desember 15, 2021
AWSConfigServiceRolePolicy— Tambahkan es:DescribeDomain, es:DescribeDomains, rds:DescribeDBParameters, and, elasticache:DescribeSnapshots	Kebijakan ini sekarang memberikan izin untuk mendapatkan detail tentang OpenSearch Layanan Amazon (OpenSearch Layanan) domain/domains dan untuk mendapatkan daftar parameter terperinci untuk grup parameter DB Amazon Relational Database Service (Amazon RDS) tertentu. Kebijakan ini juga memberikan izin untuk mendapatkan detail tentang snapshot Amazon ElastiCache .	8 September 2021

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan es:DescribeDomain, es:DescribeDomains, rds:DescribeDBParameters, and, elasticache:DescribeSnapshots	Kebijakan ini sekarang memberikan izin untuk mendapatkan detail tentang OpenSearch Layanan Amazon (OpenSearch Layanan) domain/domains dan untuk mendapatkan daftar parameter terperinci untuk grup parameter DB Amazon Relational Database Service (Amazon RDS) tertentu. Kebijakan ini juga memberikan izin untuk mendapatkan detail tentang snapshot Amazon ElastiCache .	8 September 2021

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkanlogs:ListTagsLogGroup, states:ListTagsForResource, states:ListStateMachines, states:DescribeStateMachine, dan izin tambahan untuk jenis AWS sumber daya	Kebijakan ini sekarang memberikan izin untuk mencantumkan tag untuk grup log, tag daftar untuk mesin status, dan mencantumkan semua mesin status. Kebijakan ini sekarang memberikan izin untuk mendapatkan detail tentang mesin negara. Kebijakan ini juga sekarang mendukung izin tambahan untuk Amazon EC2 Systems Manager (SSM), Amazon Elastic Container Registry, Amazon, Amazon Data Firehose, FSx Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Relational Database Service (Amazon RDS), Amazon SageMaker Route 53, Amazon AI, Layanan Pemberitahuan Sederhana Amazon,,, dan. AWS Database Migration Service AWS Global Accelerator AWS Storage Gateway	28 Juli 2021

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan logs:ListTagsLogGroup, states:ListTagsForResource, states:ListStateMachines, states:DescribeStateMachine, dan izin tambahan untuk jenis AWS sumber daya	Kebijakan ini sekarang memberikan izin untuk mencantumkan tag untuk grup log, tag daftar untuk mesin status, dan mencantumkan semua mesin status. Kebijakan ini sekarang memberikan izin untuk mendapatkan detail tentang mesin negara. Kebijakan ini juga sekarang mendukung izin tambahan untuk Amazon EC2 Systems Manager (SSM), Amazon Elastic Container Registry, Amazon, Amazon Data Firehose, FSx Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Relational Database Service (Amazon RDS), Amazon SageMaker Route 53, Amazon AI, Layanan Pemberitahuan Sederhana Amazon,,, dan. AWS Database Migration Service AWS Global Accelerator AWS Storage Gateway	28 Juli 2021

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan ssm:DescribeDocumentPermission dan izin tambahan untuk jenis AWS sumber daya	Kebijakan ini sekarang memberikan izin untuk melihat izin AWS Systems Manager dokumen dan informasi tentang IAM Access Analyzer. Kebijakan ini sekarang mendukung jenis AWS sumber daya tambahan untuk Amazon Kinesis, Amazon, Amazon EMR, ElastiCache Amazon Route 53, dan AWS Network Firewall Amazon Relational Database Service (Amazon RDS). Perubahan izin ini memungkinkan AWS Config untuk memanggil read-only yang APIs diperlukan untuk mendukung jenis sumber daya ini. Kebijakan ini juga sekarang mendukung pemfilteran fungsi Lambda @Edge untuk aturan terkelola lambda-inside-vpc AWS Config .	8 Juni 2021

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan ssm:DescribeDocumentPermission dan izin tambahan untuk jenis AWS sumber daya	Kebijakan ini sekarang memberikan izin untuk melihat izin AWS Systems Manager dokumen dan informasi tentang IAM Access Analyzer. Kebijakan ini sekarang mendukung jenis AWS sumber daya tambahan untuk Amazon Kinesis, Amazon, Amazon EMR, ElastiCache Amazon Route 53, dan AWS Network Firewall Amazon Relational Database Service (Amazon RDS). Perubahan izin ini memungkinkan AWS Config untuk memanggil read-only yang APIs diperlukan untuk mendukung jenis sumber daya ini. Kebijakan ini juga sekarang mendukung pemfilteran fungsi Lambda @Edge untuk aturan terkelola lambda-inside-vpc AWS Config .	8 Juni 2021

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan apigateway:GET izin untuk melakukan panggilan GET hanya-baca ke API Gateway dan s3:GetAccessPointPolicy izin serta s3:GetAccessPointPolicyStatus izin untuk memanggil Amazon S3 hanya-baca APIs	Kebijakan ini sekarang memberikan izin yang memungkinkan panggilan GET hanya-baca AWS Config ke API Gateway guna mendukung Aturan API Gateway. AWS Config Kebijakan ini juga menambahkan izin yang memungkinkan AWS Config untuk memanggil Amazon Simple Storage Service (Amazon S3) APIs read-only, yang diperlukan untuk mendukung jenis sumber daya baru. `AWS::S3::AccessPoint`	10 Mei 2021
AWS_COnFigRole - Tambahkan apigateway:GET izin untuk melakukan panggilan GET hanya-baca ke API Gateway dan s3:GetAccessPointPolicy izin serta izin untuk s3:GetAccessPointPolicyStatus memanggil Amazon S3 hanya-baca APIs	Kebijakan ini sekarang memberikan izin yang memungkinkan panggilan GET hanya-baca AWS Config ke API Gateway guna mendukung API AWS Config Gateway. Kebijakan ini juga menambahkan izin yang memungkinkan AWS Config untuk memanggil Amazon Simple Storage Service (Amazon S3) APIs read-only, yang diperlukan untuk mendukung jenis sumber daya baru. `AWS::S3::AccessPoint`	10 Mei 2021

Perubahan	Deskripsi	Tanggal
AWSConfigServiceRolePolicy— Tambahkan ssm:ListDocuments izin dan izin tambahan untuk jenis AWS sumber daya	Kebijakan ini sekarang memberikan izin untuk melihat informasi tentang dokumen AWS Systems Manager tertentu. Kebijakan ini juga sekarang mendukung jenis AWS sumber daya tambahan untuk AWS Backup, Amazon Elastic File System, Amazon ElastiCache, Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud EC2 (Amazon), Amazon SageMaker Kinesis, Amazon AI, dan AWS Database Migration Service Amazon Route 53. Perubahan izin ini memungkinkan AWS Config untuk memanggil read-only yang APIs diperlukan untuk mendukung jenis sumber daya ini.	1 April 2021

Perubahan	Deskripsi	Tanggal
AWS_ConfigRole— Tambahkan ssm:ListDocuments izin dan izin tambahan untuk jenis AWS sumber daya	Kebijakan ini sekarang memberikan izin untuk melihat informasi tentang dokumen AWS Systems Manager tertentu. Kebijakan ini juga sekarang mendukung jenis AWS sumber daya tambahan untuk AWS Backup, Amazon Elastic File System, Amazon ElastiCache, Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud EC2 (Amazon), Amazon SageMaker Kinesis, Amazon AI, dan AWS Database Migration Service Amazon Route 53. Perubahan izin ini memungkinkan AWS Config untuk memanggil read-only yang APIs diperlukan untuk mendukung jenis sumber daya ini.	1 April 2021
`AWSConfigRole` sudah usang	`AWSConfigRole` sudah usang. Kebijakan penggantian adalah`AWS_ConfigRole` .	1 April 2021
AWS Config mulai melacak perubahan	AWS Config mulai melacak perubahan untuk kebijakan AWS terkelolanya.	1 April 2021

Izin untuk Peran IAM Ditugaskan AWS Config

Peran IAM memungkinkan Anda menentukan satu set izin. AWS Config mengasumsikan peran yang Anda tetapkan untuk menulis ke bucket S3 Anda, mempublikasikan ke topik SNS Anda, dan membuat `Describe` atau permintaan `List` API untuk mendapatkan detail konfigurasi untuk sumber daya Anda. AWS Untuk informasi selengkapnya tentang peran IAM, lihat Peran IAM dalam Panduan Pengguna IAM.

Saat Anda menggunakan AWS Config konsol untuk membuat atau memperbarui peran IAM, AWS Config secara otomatis melampirkan izin yang diperlukan untuk Anda. Untuk informasi selengkapnya, lihat Menyiapkan AWS Config dengan Konsol.

> **Kebijakan dan hasil kepatuhan**
>
> Kebijakan IAM dan kebijakan lain yang dikelola AWS Organizations dapat memengaruhi apakah AWS Config memiliki izin untuk merekam perubahan konfigurasi untuk sumber daya Anda. Selain itu, aturan secara langsung mengevaluasi konfigurasi sumber daya dan aturan tidak memperhitungkan kebijakan ini saat menjalankan evaluasi. Pastikan bahwa kebijakan yang berlaku selaras dengan cara Anda berniat untuk menggunakan AWS Config.

Daftar Isi

- Membuat Kebijakan Peran IAM
  - Menambahkan Kebijakan Kepercayaan IAM ke Peran Anda
  - Kebijakan Peran IAM untuk Bucket S3 Anda
  - Kebijakan Peran IAM untuk Kunci KMS
  - Kebijakan Peran IAM untuk Topik Amazon SNS
  - Kebijakan Peran IAM untuk Mendapatkan Detail Konfigurasi
  - Mengelola Izin untuk Perekaman Bucket S3

Membuat Kebijakan Peran IAM

Saat Anda menggunakan AWS Config konsol untuk membuat peran IAM, AWS Config secara otomatis melampirkan izin yang diperlukan ke peran untuk Anda.

Jika Anda menggunakan AWS CLI untuk menyiapkan AWS Config atau memperbarui peran IAM yang ada, Anda harus memperbarui kebijakan secara manual agar dapat mengakses bucket S3,

memublikasikan ke topik SNS, dan mendapatkan detail konfigurasi tentang sumber daya Anda. AWS Config

Menambahkan Kebijakan Kepercayaan IAM ke Peran Anda

Anda dapat membuat kebijakan kepercayaan IAM yang memungkinkan AWS Config untuk mengambil peran dan menggunakannya untuk melacak sumber daya Anda. Untuk informasi selengkapnya tentang kebijakan kepercayaan, lihat Istilah dan konsep peran dalam Panduan Pengguna IAM.

Berikut ini adalah contoh kebijakan kepercayaan untuk AWS Config peran:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    }
  ]
}
```

Anda dapat menggunakan `AWS:SourceAccount` kondisi dalam hubungan IAM Role Trust di atas untuk membatasi prinsip layanan Config agar hanya berinteraksi dengan Peran AWS IAM saat melakukan operasi atas nama akun tertentu.

AWS Config juga mendukung `AWS:SourceArn` kondisi yang membatasi prinsipal layanan Config untuk hanya mengambil Peran IAM saat melakukan operasi atas nama akun yang memiliki. Saat menggunakan prinsip AWS Config layanan, `AWS:SourceArn` properti akan selalu disetel ke

`arn:aws:config:sourceRegion:sourceAccountID:*` wilayah `sourceRegion` perekam konfigurasi yang dikelola pelanggan dan `sourceAccountID` merupakan ID akun yang berisi perekam konfigurasi yang dikelola pelanggan.

Misalnya, tambahkan kondisi berikut, batasi prinsip layanan Config untuk hanya mengasumsikan Peran IAM hanya atas nama perekam konfigurasi yang dikelola pelanggan di wilayah `us-east-1` di akun:. `123456789012` `"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`

Kebijakan Peran IAM untuk Bucket S3 Anda

Contoh kebijakan berikut memberikan AWS Config izin untuk mengakses bucket S3 Anda:

JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/myAccountID/*"
      ],
      "Condition":{
        "StringLike":{
          "s3:x-amz-acl":"bucket-owner-full-control"
        }
      }
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:GetBucketAcl"
      ],
      "Resource":"arn:aws:s3:::amzn-s3-demo-bucket"
    }
  ]
}
```

Kebijakan Peran IAM untuk Kunci KMS

Contoh kebijakan berikut memberikan AWS Config izin untuk menggunakan enkripsi berbasis KMS pada objek baru untuk pengiriman bucket S3:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "myKMSKeyARN"
        }
    ]
}
```

Kebijakan Peran IAM untuk Topik Amazon SNS

Contoh kebijakan berikut memberikan AWS Config izin untuk mengakses topik SNS Anda:

JSON

```
{
  "Version": "2012-10-17",
  "Statement":
   [
     {
      "Effect":"Allow",
      "Action":"sns:Publish",
      "Resource":"mySNStopicARN"
     }
    ]
}
```

Jika topik SNS Anda dienkripsi untuk petunjuk penyiapan tambahan, lihat Mengonfigurasi AWS KMS Izin di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

Kebijakan Peran IAM untuk Mendapatkan Detail Konfigurasi

Disarankan untuk menggunakan peran AWS Config terkait layanan:. `AWSServiceRoleForConfig` Peran terkait layanan telah ditentukan sebelumnya dan mencakup semua izin yang AWS Config diperlukan untuk memanggil yang lain. Layanan AWS Peran AWS Config terkait layanan diperlukan untuk perekam konfigurasi terkait layanan. Untuk informasi selengkapnya, lihat Menggunakan Peran Tertaut Layanan untuk. AWS Config

Jika Anda membuat atau memperbarui peran dengan konsol, AWS Config lampirkan AWSServiceRoleForConfiguntuk Anda.

Jika Anda menggunakan AWS CLI, gunakan `attach-role-policy` perintah dan tentukan Nama Sumber Daya Amazon (ARN) untuk: AWSServiceRoleForConfig

```
$ aws iam attach-role-policy --role-name myConfigRole --policy-arn
 arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForConfig
```

Mengelola Izin untuk Perekaman Bucket S3

AWS Config merekam dan mengirimkan notifikasi saat bucket S3 dibuat, diperbarui, atau dihapus.

Disarankan untuk menggunakan peran AWS Config terkait layanan:. `AWSServiceRoleForConfig` Peran terkait layanan telah ditentukan sebelumnya dan mencakup semua izin yang AWS Config diperlukan untuk memanggil yang lain. Layanan AWS Peran AWS Config terkait layanan diperlukan untuk perekam konfigurasi terkait layanan. Untuk informasi selengkapnya, lihat Menggunakan Peran Tertaut Layanan untuk. AWS Config

Memperbarui Peran IAM untuk perekam konfigurasi terkelola pelanggan

Anda dapat memperbarui peran IAM yang digunakan oleh perekam konfigurasi terkelola pelanggan. Sebelum Anda memperbarui peran IAM, pastikan Anda telah membuat peran baru untuk menggantikan yang lama. Anda harus melampirkan kebijakan ke peran baru yang memberikan izin AWS Config untuk merekam konfigurasi dan mengirimkannya ke saluran pengiriman Anda.

Untuk informasi tentang membuat peran IAM dan melampirkan kebijakan yang diperlukan ke peran IAM, lihat. Langkah 3: Membuat Peran IAM

> **Note**
>
> Untuk menemukan ARN dari peran IAM yang ada, buka konsol IAM di. https://console.aws.amazon.com/iam/ Pilih Peran di panel navigasi. Kemudian pilih nama peran yang diinginkan dan temukan ARN di bagian atas halaman Ringkasan.

Memperbarui Peran IAM

Anda dapat memperbarui peran IAM Anda menggunakan AWS Management Console atau. AWS CLI

To update the IAM role (Console)

1. Masuk ke AWS Management Console dan buka AWS Config konsol di https://console.aws.amazon.com/config/rumah.
2. Pilih Pengaturan di panel navigasi.
3. Pada tab Perekam terkelola pelanggan, pilih Edit di halaman Pengaturan.
4. Di bagian Tata kelola data, pilih peran IAM untuk: AWS Config
   - Gunakan peran AWS Config terkait layanan yang ada — AWS Config buat peran yang memiliki izin yang diperlukan.
   - Pilih peran dari akun Anda — Untuk peran yang ada, pilih peran IAM di akun Anda.
5. Pilih Simpan.

To update the IAM role (AWS CLI)

Gunakan `put-configuration-recorder`perintah dan tentukan Nama Sumber Daya Amazon (ARN) dari peran baru:

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

Izin untuk Bucket Amazon S3 untuk AWS Config Saluran Pengiriman

> **Important**
>
> Halaman ini berisi tentang menyiapkan Amazon S3 Bucket untuk saluran AWS Config pengiriman. Halaman ini bukan tentang jenis `AWS::S3::Bucket` sumber daya yang dapat direkam oleh perekam AWS Config konfigurasi.

Bucket dan objek Amazon S3 bersifat pribadi secara default. Hanya Akun AWS yang membuat bucket (pemilik sumber daya) yang memiliki izin akses. Pemilik sumber daya dapat memberikan akses ke sumber daya dan pengguna lain dengan membuat kebijakan akses.

Saat AWS Config secara otomatis membuat bucket S3 untuk Anda, ia menambahkan izin yang diperlukan. Namun, jika Anda menentukan bucket S3 yang ada, Anda harus menambahkan izin ini secara manual.

Topik

- Izin yang Diperlukan untuk Bucket Amazon S3 Saat Menggunakan Peran IAM
- Izin yang Diperlukan untuk Bucket Amazon S3 Saat Menggunakan Peran Tertaut Layanan
- Memberikan AWS Config akses ke Amazon S3 Bucket
- Izin yang Diperlukan untuk Bucket Amazon S3 Saat Mengirimkan Lintas Akun

Izin yang Diperlukan untuk Bucket Amazon S3 Saat Menggunakan Peran IAM

AWS Config menggunakan peran IAM yang Anda tetapkan ke perekam konfigurasi untuk mengirimkan riwayat konfigurasi dan snapshot ke bucket S3 di akun Anda. Untuk pengiriman lintas akun, upaya AWS Config pertama untuk menggunakan peran IAM yang ditetapkan. Jika kebijakan bucket tidak memberikan `WRITE` akses ke peran IAM, AWS Config gunakan prinsip `config.amazonaws.com` layanan. Kebijakan bucket harus memberikan `WRITE` akses `config.amazonaws.com` untuk menyelesaikan pengiriman. Setelah pengiriman berhasil, AWS Config pertahankan kepemilikan semua objek yang dikirimkan ke bucket S3 lintas akun.

AWS Config memanggil Amazon S3 HeadBucketAPI dengan peran IAM yang Anda tetapkan ke perekam konfigurasi untuk mengonfirmasi apakah bucket S3 ada dan lokasinya. Jika Anda tidak memiliki izin yang diperlukan AWS Config untuk mengonfirmasi, Anda akan melihat `AccessDenied`

kesalahan di AWS CloudTrail log Anda. Namun, masih AWS Config dapat mengirimkan riwayat konfigurasi dan snapshot meskipun AWS Config tidak memiliki izin yang diperlukan untuk mengonfirmasi apakah bucket S3 ada dan lokasinya.

> **Izin minimum**
>
> `HeadBucket`API Amazon S3 memerlukan tindakan. `s3:ListBucket`

Izin yang Diperlukan untuk Bucket Amazon S3 Saat Menggunakan Peran Tertaut Layanan

Peran AWS Config terkait layanan tidak memiliki izin untuk menempatkan objek ke bucket Amazon S3. Jika Anda mengatur AWS Config menggunakan peran terkait layanan, AWS Config akan menggunakan prinsip `config.amazonaws.com` layanan untuk memberikan riwayat konfigurasi dan snapshot. Kebijakan bucket S3 di akun atau tujuan lintas akun Anda harus menyertakan izin bagi prinsipal AWS Config layanan untuk menulis objek.

Memberikan AWS Config akses ke Amazon S3 Bucket

Selesaikan langkah-langkah berikut yang memungkinkan AWS Config untuk mengirimkan riwayat konfigurasi dan snapshot ke bucket Amazon S3.

1. Masuk ke akun AWS Management Console menggunakan akun yang memiliki bucket S3.
2. Buka konsol Amazon S3 di. https://console.aws.amazon.com/s3/
3. Pilih bucket yang ingin Anda gunakan AWS Config untuk mengirimkan item konfigurasi, lalu pilih Properties.
4. Pilih Izin.
5. Pilih Edit Kebijakan Bucket.
6. Salin kebijakan berikut ke jendela Bucket Policy Editor:

> **Praktik terbaik keamanan**
>
> Kami sangat menyarankan Anda membatasi akses dalam kebijakan bucket dengan `AWS:SourceAccount` kondisi tersebut. Hal ini memastikan bahwa AWS Config diberikan akses atas nama pengguna yang diharapkan saja.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    },
    {
      "Sid": "AWSConfigBucketExistenceCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    },
    {
      "Sid": "AWSConfigBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:PutObject",
```

```
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/[optional] prefix/
AWSLogs/sourceAccountID/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    }
  ]
}
```

7. Ganti nilai berikut dalam kebijakan bucket:
   - *amzn-s3-demo-bucket*— Nama bucket Amazon S3 tempat AWS Config akan memberikan riwayat konfigurasi dan snapshot.
   - *[optional] prefix*— Tambahan opsional untuk kunci objek Amazon S3 yang membantu membuat organisasi seperti folder di bucket.
   - *sourceAccountID*— ID akun tempat AWS Config akan memberikan riwayat konfigurasi dan snapshot.
8. Pilih Simpan dan kemudian Tutup.

`AWS:SourceAccount`Kondisi ini membatasi AWS Config operasi untuk ditentukan Akun AWS. Untuk konfigurasi multi-akun dalam organisasi yang mengirimkan ke satu bucket S3, gunakan peran IAM dengan kunci AWS Organizations kondisi, bukan peran terkait layanan. Misalnya, `AWS:PrincipalOrgID`. Untuk informasi selengkapnya, lihat Mengelola izin akses untuk organisasi di Panduan AWS Organizations pengguna.

`AWS:SourceArn`Kondisi ini membatasi AWS Config operasi ke saluran pengiriman tertentu. `AWS:SourceArn`Formatnya adalah sebagai berikut:`arn:aws:config:`*sourceRegion*`:`*123456789012*.

Misalnya, untuk membatasi akses bucket S3 ke saluran pengiriman di Wilayah AS Timur (Virginia N.) untuk akun 123456789012, tambahkan kondisi berikut:

```
"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:"}
```

Izin yang Diperlukan untuk Bucket Amazon S3 Saat Mengirimkan Lintas Akun

Bila AWS Config dikonfigurasi untuk mengirimkan riwayat konfigurasi dan snapshot ke bucket Amazon S3 di akun lain (penyiapan lintas akun), di mana perekam konfigurasi dan bucket S3 yang ditentukan untuk saluran pengiriman Akun AWS berbeda, izin berikut diperlukan:

- Peran IAM yang Anda tetapkan ke perekam konfigurasi memerlukan izin eksplisit untuk melakukan operasi. `s3:ListBucket` Ini karena AWS Config memanggil HeadBucketAPI Amazon S3 dengan peran IAM ini untuk menentukan lokasi bucket.
- Kebijakan bucket S3 harus menyertakan izin untuk prinsipal AWS Config layanan dan peran IAM yang ditetapkan ke perekam konfigurasi.

Berikut ini adalah contoh konfigurasi kebijakan bucket:

```
{
      "Sid": "AWSConfigBucketExistenceCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com",
        "AWS": "IAM Role-Arn assigned to the configuration recorder"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
}
```

Izin untuk Kunci KMS untuk Saluran Pengiriman AWS Config

Gunakan informasi dalam topik ini jika Anda ingin membuat kebijakan untuk AWS KMS kunci bucket S3 yang memungkinkan Anda menggunakan enkripsi berbasis KMS pada objek yang dikirimkan AWS Config untuk pengiriman bucket S3.

Daftar Isi

- Izin yang Diperlukan untuk Kunci KMS Saat Menggunakan Peran IAM (Pengiriman Bucket S3)

- Izin yang Diperlukan untuk AWS KMS Kunci Saat Menggunakan Peran Tertaut Layanan (Pengiriman Bucket S3)
- Memberikan AWS Config akses ke Kunci AWS KMS

Izin yang Diperlukan untuk Kunci KMS Saat Menggunakan Peran IAM (Pengiriman Bucket S3)

Jika Anda mengatur AWS Config menggunakan peran IAM, Anda dapat melampirkan kebijakan izin ikuti ke Kunci KMS:

```
{
    "Id": "Policy_ID",
    "Statement": [
        {
            "Sid": "AWSConfigKMSPolicy",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Effect": "Allow",
            "Resource": "*myKMSKeyARN*",
            "Principal": {
                "AWS": [
                    "account-id1",
                    "account-id2",
                    "account-id3"
                ]
            }
        }
    ]
}
```

> **Note**
>
> Jika peran IAM, kebijakan bucket Amazon S3, AWS KMS atau kunci tidak memberikan akses yang sesuai, AWS Config maka upaya AWS Config untuk mengirim informasi konfigurasi ke bucket Amazon S3 akan gagal. Dalam acara ini, AWS Config mengirimkan informasi lagi, kali ini sebagai kepala AWS Config layanan. Untuk kasus ini, Anda harus melampirkan kebijakan

izin, yang disebutkan di bawah ini, ke AWS KMS kunci untuk memberikan AWS Config akses untuk menggunakan kunci saat mengirimkan informasi ke bucket Amazon S3.

Izin yang Diperlukan untuk AWS KMS Kunci Saat Menggunakan Peran Tertaut Layanan (Pengiriman Bucket S3)

Peran AWS Config terkait layanan tidak memiliki izin untuk mengakses kunci. AWS KMS Jadi, jika Anda mengatur AWS Config menggunakan peran terkait layanan, AWS Config akan mengirim informasi sebagai prinsipal AWS Config layanan sebagai gantinya. Anda harus melampirkan kebijakan akses, yang disebutkan di bawah ini, ke AWS KMS kunci untuk memberikan AWS Config akses untuk menggunakan AWS KMS kunci saat mengirimkan informasi ke bucket Amazon S3.

Memberikan AWS Config akses ke Kunci AWS KMS

Kebijakan ini memungkinkan AWS Config untuk menggunakan AWS KMS kunci saat mengirimkan informasi ke bucket Amazon S3

```
{
    "Id": "Policy_ID",
    "Statement": [
        {
            "Sid": "AWSConfigKMSPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "myKMSKeyARN",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceAccount": "sourceAccountID"
                }
            }
        }
    ]
}
```

Gantikan nilai-nilai berikut dalam kebijakan kunci:

- *myKMSKeyARN*— ARN AWS KMS kunci yang digunakan untuk mengenkripsi data di bucket Amazon S3 yang AWS Config akan mengirimkan item konfigurasi ke.
- *sourceAccountID*— ID akun yang AWS Config akan mengirimkan item konfigurasi ke.

Anda dapat menggunakan `AWS:SourceAccount` kondisi dalam kebijakan AWS KMS utama di atas untuk membatasi prinsip layanan Config agar hanya berinteraksi dengan AWS KMS kunci saat melakukan operasi atas nama akun tertentu.

AWS Config juga mendukung `AWS:SourceArn` kondisi yang membatasi prinsip layanan Config untuk hanya berinteraksi dengan bucket Amazon S3 saat melakukan operasi atas nama saluran pengiriman tertentu. AWS Config Saat menggunakan prinsip AWS Config layanan, `AWS:SourceArn` properti akan selalu diatur ke `arn:aws:config:sourceRegion:sourceAccountID:*` mana `sourceRegion` wilayah saluran pengiriman dan `sourceAccountID` merupakan ID akun yang berisi saluran pengiriman. Untuk informasi selengkapnya tentang saluran AWS Config pengiriman, lihat Mengelola Saluran Pengiriman. Misalnya, tambahkan kondisi berikut untuk membatasi prinsip layanan Config agar berinteraksi dengan bucket Amazon S3 Anda hanya atas nama saluran pengiriman di wilayah `us-east-1` di akun:. `123456789012` `"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`

Izin untuk Topik Amazon SNS

Topik ini menjelaskan cara mengonfigurasi AWS Config untuk mengirimkan topik Amazon SNS yang dimiliki oleh akun lain. AWS Config harus memiliki izin yang diperlukan untuk mengirim pemberitahuan ke topik Amazon SNS.

Saat AWS Config konsol membuat topik Amazon SNS baru untuk Anda, AWS Config berikan izin yang diperlukan. Jika Anda memilih topik Amazon SNS yang ada, pastikan bahwa topik Amazon SNS menyertakan izin yang diperlukan dan mengikuti praktik terbaik keamanan.

> **Topik Amazon SNS Lintas Wilayah tidak didukung**
>
> AWS Config saat ini hanya mendukung akses dalam akun yang sama Wilayah AWS dan di seluruh akun.

Daftar Isi

- Izin yang Diperlukan untuk Topik Amazon SNS Saat Menggunakan Peran IAM
- Izin yang Diperlukan untuk Topik Amazon SNS Saat Menggunakan Peran Tertaut Layanan
- Memberikan AWS Config akses ke topik Amazon SNS
- Pemecahan Masalah untuk Topik Amazon SNS

Izin yang Diperlukan untuk Topik Amazon SNS Saat Menggunakan Peran IAM

Anda dapat melampirkan kebijakan izin ke topik Amazon SNS yang dimiliki oleh akun lain. Jika Anda ingin menggunakan topik Amazon SNS dari akun lain, pastikan untuk melampirkan kebijakan berikut ke topik Amazon SNS yang ada.

```
{
  "Id": "Policy_ID",
  "Statement": [
    {
      "Sid": "AWSConfigSNSPolicy",
      "Action": [
        "sns:Publish"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
      "Principal": {
        "AWS": [
          "account-id1",
          "account-id2",
          "account-id3"
        ]
      }
    }
  ]
}
```

Untuk `Resource` kuncinya, *`account-id`* adalah nomor AWS akun pemilik topik. Untuk*`account-id1`*,*`account-id2`*, dan*`account-id3`*, gunakan Akun AWS yang akan mengirim data ke topik Amazon SNS. Anda dapat mengganti nilai yang sesuai untuk *`region`* dan*`myTopic`*.

Saat AWS Config mengirim pemberitahuan ke topik Amazon SNS, pertama kali mencoba menggunakan peran IAM, tetapi upaya ini gagal jika peran atau Akun AWS tidak memiliki izin untuk mempublikasikan ke topik tersebut. Dalam hal ini, AWS Config kirimkan notifikasi lagi, kali ini sebagai AWS Config service principal name (SPN). Sebelum publikasi berhasil, kebijakan akses untuk topik

harus memberikan `sns:Publish` akses ke nama `config.amazonaws.com` utama. Anda harus melampirkan kebijakan akses, yang dijelaskan di bagian berikutnya, ke topik Amazon SNS untuk memberikan AWS Config akses ke topik Amazon SNS jika peran IAM tidak memiliki izin untuk mempublikasikan ke topik tersebut.

Izin yang Diperlukan untuk Topik Amazon SNS Saat Menggunakan Peran Tertaut Layanan

Peran AWS Config terkait layanan tidak memiliki izin untuk mengakses topik Amazon SNS. Jadi, jika Anda mengatur AWS Config menggunakan peran terkait layanan (SLR), AWS Config akan mengirim informasi sebagai prinsipal AWS Config layanan sebagai gantinya. Anda harus melampirkan kebijakan akses, yang disebutkan di bawah ini, ke topik Amazon SNS untuk memberikan AWS Config akses untuk mengirim informasi ke topik Amazon SNS.

Untuk pengaturan akun yang sama, ketika topik Amazon SNS dan SLR berada di akun yang sama dan kebijakan Amazon SNS memberikan izin `sns:Publish` “” SLR, Anda tidak perlu menggunakan SPN. AWS Config Kebijakan izin di bawah ini dan rekomendasi praktik terbaik keamanan adalah untuk penyiapan lintas akun.

Memberikan AWS Config akses ke topik Amazon SNS

Kebijakan ini memungkinkan AWS Config untuk mengirim pemberitahuan ke topik Amazon SNS. Untuk memberikan AWS Config akses ke topik Amazon SNS dari akun lain, Anda harus melampirkan kebijakan izin berikut.

> **Note**
>
> Sebagai praktik keamanan terbaik, sangat disarankan untuk memastikan AWS Config mengakses sumber daya atas nama pengguna yang diharapkan hanya dengan membatasi akses ke akun yang tercantum dalam `AWS:SourceAccount` kondisi.

```
{
"Id": "Policy_ID",
"Statement": [
  {
    "Sid": "AWSConfigSNSPolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "config.amazonaws.com"
```

```
    },
    "Action": "sns:Publish",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
        "Condition" : {
        "StringEquals": {
          "AWS:SourceAccount": [
            "account-id1",
            "account-id2",
            "account-id3"
          ]
        }
      }
    }
  ]
}
```

Untuk `Resource` kuncinya, *`account-id`* adalah nomor AWS akun pemilik topik. Untuk*`account-id1`*,*`account-id2`*, dan*`account-id3`*, gunakan Akun AWS yang akan mengirim data ke topik Amazon SNS. Anda dapat mengganti nilai yang sesuai untuk *`region`* dan*`myTopic`*.

Anda dapat menggunakan `AWS:SourceAccount` kondisi dalam kebijakan topik Amazon SNS sebelumnya untuk membatasi nama utama AWS Config layanan (SPN) agar hanya berinteraksi dengan topik Amazon SNS saat melakukan operasi atas nama akun tertentu.

AWS Config juga mendukung `AWS:SourceArn` kondisi yang membatasi nama utama AWS Config layanan (SPN) untuk hanya berinteraksi dengan bucket S3 saat melakukan operasi atas nama saluran pengiriman tertentu AWS Config . Saat menggunakan nama utama AWS Config layanan (SPN), `AWS:SourceArn` properti akan selalu diatur ke `arn:aws:config:sourceRegion:sourceAccountID:*` mana `sourceRegion` adalah Wilayah saluran pengiriman dan `sourceAccountID` merupakan ID akun yang berisi saluran pengiriman. Untuk informasi selengkapnya tentang saluran AWS Config pengiriman, lihat Mengelola Saluran Pengiriman. Misalnya, tambahkan kondisi berikut untuk membatasi nama utama AWS Config layanan (SPN) agar berinteraksi dengan bucket S3 Anda hanya atas nama saluran pengiriman di `us-east-1` Wilayah di akun:. `123456789012` `"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`

Pemecahan Masalah untuk Topik Amazon SNS

AWS Config harus memiliki izin untuk mengirim pemberitahuan ke topik Amazon SNS. Jika topik Amazon SNS tidak dapat menerima pemberitahuan, verifikasi bahwa peran IAM yang AWS Config diasumsikan memiliki izin yang diperlukan. `sns:Publish`

Memecahkan masalah AWS Config identitas dan akses

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan AWS Config dan IAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di AWS Config
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses AWS Config sumber daya saya

Saya tidak berwenang untuk melakukan tindakan di AWS Config

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh kesalahan berikut terjadi ketika pengguna IAM `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang suatu sumber daya fiktif *`my-example-widget`*, tetapi tidak memiliki izin fiktif `config:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 config:GetWidget on resource: my-example-widget
```

Dalam hal ini, kebijakan Mateo harus diperbarui untuk memungkinkannya mengakses *`my-example-widget`* sumber daya menggunakan `config:`*`GetWidget`* tindakan.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan yang tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran AWS Config.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol tersebut untuk melakukan tindakan di AWS Config. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses AWS Config sumber daya saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACLs), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mempelajari apakah AWS Config mendukung fitur-fitur ini, lihatBagaimana AWS Config bekerja dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

Menggunakan Peran Tertaut Layanan untuk AWS Config

AWS Config menggunakan AWS Identity and Access Management peran terkait layanan (IAM). Peran terkait layanan adalah jenis unik peran IAM yang ditautkan langsung ke. AWS Config Peran terkait layanan telah ditentukan sebelumnya oleh AWS Config dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan membuat pengaturan AWS Config lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. AWS Config mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya AWS Config dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat Layanan AWS yang Berfungsi dengan IAM dan cari layanan yang memiliki Ya di kolom Peran Terkait Layanan. Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Izin Peran Tertaut Layanan untuk AWS Config

AWS Config menggunakan peran terkait layanan bernama AwsServiceRoleForConfig— AWS Config menggunakan peran terkait layanan ini untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan AwsServiceRoleForConfig memercayai layanan `config.amazonaws.com` untuk menjalankan peran.

Kebijakan izin untuk `AwsServiceRoleForConfig` peran tersebut berisi izin hanya-baca dan hanya tulis untuk sumber daya dan izin hanya-baca untuk AWS Config sumber daya di layanan lain yang mendukung. AWS Config Untuk melihat kebijakan terkelola AwsServiceRoleForConfig, lihat kebijakan AWS terkelola untuk AWS Config.

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, silakan lihat Izin Peran Tertaut Layanan di Panduan Pengguna IAM.

Untuk menggunakan peran terkait layanan AWS Config, Anda harus mengonfigurasi izin di bucket Amazon S3 dan topik Amazon SNS. Lihat informasi selengkapnya di Izin yang Diperlukan untuk Bucket Amazon S3 Saat Menggunakan Peran Tertaut Layanan, Izin yang Diperlukan untuk AWS KMS Kunci Saat Menggunakan Peran Tertaut Layanan (Pengiriman Bucket S3), dan Izin yang Diperlukan untuk Topik Amazon SNS Saat Menggunakan Peran Tertaut Layanan.

Membuat Peran Tertaut Layanan untuk AWS Config

Di IAM CLI atau IAM API, buat peran tertaut layanan dengan nama layanan `config.amazonaws.com`. Untuk informasi lebih lanjut, lihat Membuat Peran yang Terhubung dengan Layanan di Panduan Pengguna IAM. Jika Anda menghapus peran tertaut layanan ini, Anda dapat mengulang proses yang sama untuk membuat peran tersebut lagi.

Mengedit Peran Tertaut Layanan untuk AWS Config

AWS Config tidak memungkinkan Anda untuk mengedit peran AwsServiceRoleForConfigterkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin merujuk peran tersebut. Namun, Anda dapat mengedit penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit Peran Tertaut Layanan dalam Panduan Pengguna IAM.

Menghapus Peran Tertaut Layanan untuk AWS Config

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, sebaiknya hapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif. Tetapi, Anda harus membersihkan sumber daya peran yang terhubung dengan layanan sebelum menghapusnya secara manual.

> **Note**
>
> Jika AWS Config layanan menggunakan peran saat Anda mencoba menghapus sumber daya, maka penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus AWS Config sumber daya yang digunakan oleh AwsServiceRoleForConfig

Pastikan Anda tidak `ConfigurationRecorders` menggunakan peran terkait layanan. Anda dapat menggunakan AWS Config konsol untuk menghentikan perekam konfigurasi. Untuk berhenti merekam, di bawah Perekaman aktif, pilih Matikan.

Anda dapat menghapus `ConfigurationRecorder` menggunakan AWS Config API. Untuk menghapus, gunakan `delete-configuration-recorder` perintah.

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

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, CLI IAM, atau API CLI untuk menghapus peran tertaut layanan AwsServiceRoleForConfig. Untuk informasi selengkapnya, lihat Menghapus Peran Terkait Layanan di Panduan Pengguna IAM.

Respon Insiden di AWS Config

Keamanan adalah prioritas tertinggi di AWS. Sebagai bagian dari model tanggung jawab bersama AWS Cloud, AWS mengelola pusat data, jaringan, dan arsitektur perangkat lunak yang memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan. AWS bertanggung jawab atas setiap respons insiden sehubungan dengan AWS Config layanan itu sendiri. Selain itu, sebagai AWS pelanggan, Anda berbagi tanggung jawab untuk menjaga keamanan di cloud. Ini berarti Anda mengontrol keamanan yang Anda pilih untuk diterapkan dari AWS alat dan fitur yang dapat Anda akses, dan bertanggung jawab atas respons insiden di pihak Anda dari model tanggung jawab bersama.

Dengan menetapkan garis dasar keamanan yang memenuhi tujuan aplikasi Anda yang berjalan di cloud, Anda dapat mendeteksi penyimpangan yang dapat Anda tanggapi. Karena respons insiden keamanan dapat menjadi topik yang kompleks, kami mendorong Anda untuk meninjau sumber daya berikut sehingga Anda lebih dapat memahami dampak respons insiden (IR) dan pilihan Anda terhadap tujuan perusahaan Anda: Panduan Respons Insiden AWS Keamanan, whitepaper Praktik AWS Keamanan Terbaik, dan white paper Perspektif Keamanan AWS Cloud Adoption Framework (CAF).

Validasi Kepatuhan untuk AWS Config

Auditor pihak ketiga menilai keamanan dan kepatuhan AWS Config sebagai bagian dari beberapa program AWS kepatuhan. Program ini mencakup SOC, PCI, FedRAMP, HIPAA, dan lainnya.

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Kepatuhan dan Tata Kelola Keamanan – Panduan implementasi solusi ini membahas pertimbangan arsitektur serta memberikan langkah-langkah untuk menerapkan fitur keamanan dan kepatuhan.
- Referensi Layanan yang Memenuhi Syarat HIPAA — Daftar layanan yang memenuhi syarat HIPAA. Tidak semua memenuhi Layanan AWS syarat HIPAA.
- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- Amazon GuardDuty — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- AWS Audit ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Ketahanan di AWS Config

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. AWS Wilayah menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Availability Zone, Anda dapat mendesain dan mengoperasikan aplikasi dan basis data yang secara otomatis mengalami kegagalan di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang AWS Wilayah dan Availability Zone, lihat Infrastruktur AWS Global.

Keamanan Infrastruktur di AWS Config

Sebagai layanan terkelola, AWS Config dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat Keamanan AWS Cloud. Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses AWS Config melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan prinsipal IAM. Atau Anda dapat menggunakan AWS Security Token Service (AWS STS) untuk menghasilkan kredensial keamanan sementara untuk menandatangani permintaan.

Analisis Konfigurasi dan Kelemahan

Untuk AWS Config, AWS menangani tugas-tugas keamanan dasar seperti sistem operasi tamu (OS) dan patch database, konfigurasi firewall, dan pemulihan bencana.

Pencegahan "confused deputy" lintas layanan

Masalah "confused deputy" adalah masalah keamanan saat entitas yang tidak memiliki izin untuk melakukan suatu tindakan dapat memaksa entitas yang memilik hak akses lebih tinggi untuk melakukan tindakan tersebut. Pada tahun AWS, peniruan lintas layanan dapat mengakibatkan masalah wakil yang membingungkan. Peniruan identitas lintas layanan dapat terjadi ketika satu layanan (layanan yang dipanggil) memanggil layanan lain (layanan yang dipanggil). Layanan pemanggilan dapat dimanipulasi menggunakan izinnya untuk bertindak pada sumber daya pelanggan lain dengan cara yang seharusnya tidak dilakukannya kecuali bila memiliki izin untuk mengakses. Untuk mencegah hal ini, AWS menyediakan alat yang membantu Anda melindungi data untuk semua layanan dengan principal layanan yang telah diberi akses ke sumber daya di akun Anda.

Sebaiknya gunakan kunci konteks kondisi `aws:SourceAccount`global `aws:SourceArn`dan dalam kebijakan sumber daya untuk membatasi izin yang AWS Config memberikan layanan lain ke sumber daya. Gunakan `aws:SourceArn` jika Anda ingin hanya satu sumber daya yang akan dikaitkan dengan akses lintas layanan. Gunakan `aws:SourceAccount` jika Anda ingin mengizinkan sumber daya apa pun di akun tersebut dikaitkan dengan penggunaan lintas layanan.

Cara paling efektif untuk melindungi dari masalah "confused deputy" adalah dengan menggunakan kunci konteks kondisi global `aws:SourceArn` dengan ARN lengkap sumber daya. Jika Anda tidak mengetahui ARN lengkap sumber daya atau jika Anda menentukan beberapa sumber daya, gunakan kunci kondisi konteks global `aws:SourceArn` dengan karakter wildcard (`*`) untuk bagian ARN yang tidak diketahui. Misalnya, `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`.

Jika nilai `aws:SourceArn` tidak berisi ID akun, seperti ARN bucket Amazon S3, Anda harus menggunakan kedua kunci konteks kondisi global tersebut untuk membatasi izin.

Contoh berikut menunjukkan bagaimana Anda dapat menggunakan kunci konteks kondisi `aws:SourceAccount` global `aws:SourceArn` dan AWS Config untuk mencegah masalah deputi yang membingungkan: Memberikan AWS Config akses ke Bucket Amazon S3.

Praktik Terbaik Keamanan untuk AWS Config

AWS Config menyediakan sejumlah fitur keamanan untuk dipertimbangkan saat Anda mengembangkan dan menerapkan kebijakan keamanan Anda sendiri. Praktik terbaik berikut adalah pedoman umum dan tidak mewakili solusi keamanan yang lengkap. Karena praktik terbaik ini mungkin tidak sesuai atau tidak memadai untuk lingkungan Anda, perlakukan itu sebagai pertimbangan yang bermanfaat, bukan sebagai resep.

- Manfaatkan penandaan AWS Config, yang membuat lebih mudah untuk mengelola, mencari, dan memfilter sumber daya.
- Konfirmasikan saluran pengiriman Anda telah diatur dengan benar, dan setelah dikonfirmasi, verifikasi bahwa saluran AWS Config tersebut merekam dengan benar.

Untuk informasi selengkapnya, lihat blog praktik AWS Config terbaik.

Logging dan Monitoring di AWS Config

AWS Config terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di AWS Config. Pemantauan adalah bagian penting dari menjaga keandalan, ketersediaan, dan kinerja AWS Config dan AWS solusi Anda.

Topik

- Pencatatan Panggilan AWS Config API dengan AWS CloudTrail
- Pemantauan

Pencatatan Panggilan AWS Config API dengan AWS CloudTrail

CloudTrail menangkap semua panggilan API untuk AWS Config sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari AWS Config konsol dan panggilan kode ke operasi AWS Config API. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara berkelanjutan ke bucket Amazon S3, termasuk acara untuk. AWS Config Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat AWS Config, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

Topik

- AWS Config Informasi di CloudTrail
- Memahami Entri File AWS Config Log
- Contoh File Log

AWS Config Informasi di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi di AWS Config, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di situs Anda Akun AWS. Untuk informasi selengkapnya, lihat Melihat Acara dengan Riwayat CloudTrail Acara.

Untuk catatan acara yang sedang berlangsung di Anda Akun AWS, termasuk acara untuk AWS Config, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- Gambaran Umum untuk Membuat Jejak
- CloudTrail Layanan dan Integrasi yang Didukung
- Mengkonfigurasi Notifikasi Amazon SNS untuk CloudTrail
- Menerima File CloudTrail Log dari Beberapa Wilayah dan Menerima File CloudTrail Log dari Beberapa Akun

Semua AWS Config operasi dicatat oleh CloudTrail dan didokumentasikan dalam Referensi AWS Config API. Misalnya, panggilan ke DeliverConfigSnapshot, DeleteDeliveryChannel, dan DescribeDeliveryChannelsoperasi menghasilkan entri dalam file CloudTrail log.

Setiap entri peristiwa atau log berisi informasi tentang entitas yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan hal berikut ini:

- Apakah permintaan itu dibuat dengan kredenal pengguna root atau AWS Identity and Access Management (IAM).
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi lain, lihat Elemen userIdentity CloudTrail .

Memahami Entri File AWS Config Log

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Contoh File Log

Untuk contoh entri CloudTrail log, lihat topik berikut.

DeleteDeliveryChannel

Berikut ini adalah contoh file CloudTrail log untuk DeleteDeliveryChannel operasi.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:32:57Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DeleteDeliveryChannel",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-internal/3",
      "requestParameters": {
        "deliveryChannelName": "default"
      },
      "responseElements": null,
      "requestID": "207d695a-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "5dcff7a9-e414-411a-a43e-88d122a0ad4a",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

DeliverConfigSnapshot

Berikut ini adalah contoh file CloudTrail log untuk DeliverConfigSnapshot operasi.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAABCDEFGHIJKLNMOPQ:Config-API-Test",
```

```
        "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-12-11T00:58:42Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDAABCDEFGHIJKLNMOPQ",
            "arn": "arn:aws:iam::111111111111:role/JaneDoe",
            "accountId": "111111111111",
            "userName": "JaneDoe"
          }
        }
      },
      "eventTime": "2014-12-11T00:58:53Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DeliverConfigSnapshot",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "deliveryChannelName": "default"
      },
      "responseElements": {
        "configSnapshotId": "58d50f10-212d-4fa4-842e-97c614da67ce"
      },
      "requestID": "e0248561-80d0-11e4-9f1c-7739d36a3df2",
      "eventID": "3e88076c-eae1-4aa6-8990-86fe52aedbd8",
      "eventType": "AwsApiCall",
      recipientAccountId": "111111111111"
    }
```

DescribeConfigurationRecorderStatus

Berikut ini adalah contoh file CloudTrail log untuk DescribeConfigurationRecorderStatusoperasi.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
```

```
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:44Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeConfigurationRecorderStatus",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "8442f25d-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "a675b36b-455f-4e18-a4bc-d3e01749d3f1",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

DescribeConfigurationRecorders

Berikut ini adalah contoh file CloudTrail log untuk DescribeConfigurationRecordersoperasi.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:34:52Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeConfigurationRecorders",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "6566b55c-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "6259a9ad-889e-423b-beeb-6e1eec84a8b5",
      "eventType": "AwsApiCall",
```

```
      "recipientAccountId": "222222222222"
    }
```

DescribeDeliveryChannels

Berikut ini adalah contoh file CloudTrail log untuk DescribeDeliveryChannelsoperasi.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:02Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeDeliveryChannels",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "6b6aee3f-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "3e15ebc5-bf39-4d2a-8b64-9392807985f1",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

GetResourceConfigHistory

Berikut ini adalah contoh file CloudTrail log untuk GetResourceConfigHistoryoperasi.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAABCDEFGHIJKLNMOPQ:Config-API-Test",
        "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-12-11T00:58:42Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDAABCDEFGHIJKLNMOPQ",
            "arn": "arn:aws:iam::111111111111:role/JaneDoe",
            "accountId": "111111111111",
            "userName": "JaneDoe"
          }
        }
      },
      "eventTime": "2014-12-11T00:58:42Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "GetResourceConfigHistory",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "resourceId": "vpc-a12bc345",
        "resourceType": "AWS::EC2::VPC",
        "limit": 0,
        "laterTime": "Dec 11, 2014 12:58:42 AM",
        "earlierTime": "Dec 10, 2014 4:58:42 PM"
      },
      "responseElements": null,
      "requestID": "d9f3490d-80d0-11e4-9f1c-7739d36a3df2",
      "eventID": "ba9c1766-d28f-40e3-b4c6-3ffb87dd6166",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111111111111"
      }
```

PutConfigurationRecorder

Berikut ini adalah contoh file CloudTrail log untuk PutConfigurationRecorderoperasi.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
```

```
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:23Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "PutConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorder": {
          "name": "default",
          "roleARN": "arn:aws:iam::222222222222:role/config-role-pdx"
        }
      },
      "responseElements": null,
      "requestID": "779f7917-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "c91f3daa-96e8-44ee-8ddd-146ac06565a7",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

PutDeliveryChannel

Berikut ini adalah contoh file CloudTrail log untuk PutDeliveryChannelloperasi.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:33:08Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "PutDeliveryChannel",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
```

```
        "deliveryChannel": {
          "name": "default",
          "s3BucketName": "config-api-test-pdx",
          "snsTopicARN": "arn:aws:sns:us-west-2:222222222222:config-api-test-pdx"
        }
      },
      "responseElements": null,
      "requestID": "268b8d4d-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "b2db05f1-1c73-4e52-b238-db69c04e8dd4",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

StartConfigurationRecorder

Berikut ini adalah contoh file CloudTrail log untuk StartConfigurationRecorderoperasi.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:34Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "StartConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorderName": "default"
      },
      "responseElements": null,
      "requestID": "7e03fa6a-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "55a5507f-f306-4896-afe3-196dc078a88d",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

StopConfigurationRecorder

Berikut ini adalah contoh file CloudTrail log untuk StopConfigurationRecorderoperasi.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:13Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "StopConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorderName": "default"
      },
      "responseElements": null,
      "requestID": "716deea3-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "6225a85d-1e49-41e9-bf43-3cfc5549e560",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

Pemantauan

Anda dapat menggunakan AWS layanan lain untuk memantau AWS Config sumber daya.

- Anda dapat menggunakan Amazon Simple Notification Service (SNS) untuk mengirimkan notifikasi kepada Anda setiap kali AWS sumber daya yang didukung dibuat, diperbarui, atau dimodifikasi sebagai akibat dari aktivitas API pengguna.
- Anda dapat menggunakan Amazon EventBridge untuk mendeteksi dan bereaksi terhadap perubahan status AWS Config peristiwa.

Topik

- Memantau Perubahan AWS Sumber Daya dengan Amazon SQS
- Pemantauan AWS Config dengan Amazon EventBridge

Memantau Perubahan AWS Sumber Daya dengan Amazon SQS

AWS Config menggunakan Amazon Simple Notification Service (SNS) untuk mengirimi Anda notifikasi setiap kali AWS sumber daya yang didukung dibuat, diperbarui, atau diubah sebagai hasil dari aktivitas API pengguna. Namun, Anda mungkin tertarik hanya pada perubahan konfigurasi sumber daya tertentu. Misalnya, Anda mungkin menganggap penting untuk mengetahui kapan seseorang memodifikasi konfigurasi grup keamanan, tetapi tidak perlu tahu setiap kali ada perubahan pada tag di EC2 instans Amazon Anda. Atau, Anda mungkin ingin menulis program yang melakukan tindakan tertentu saat sumber daya tertentu diperbarui. Misalnya, Anda mungkin ingin memulai alur kerja tertentu saat konfigurasi grup keamanan diubah. Jika Anda ingin menggunakan data secara terprogram dari AWS Config cara ini atau cara lain, gunakan antrean Amazon Simple Queue Service sebagai titik akhir notifikasi untuk Amazon SNS.

> **Note**
>
> Notifikasi juga dapat berasal dari Amazon SNS dalam bentuk email, pesan Short Message Service (SMS) ke ponsel dan smartphone berkemampuan SMS, pesan notifikasi ke aplikasi di perangkat seluler, atau pesan notifikasi ke satu atau beberapa titik akhir HTTP atau HTTPS.

Anda dapat memiliki satu antrian SQS berlangganan ke beberapa topik, apakah Anda memiliki satu topik untuk setiap wilayah atau satu topik untuk setiap akun untuk setiap wilayah. Anda harus berlangganan antrian ke topik SNS yang Anda inginkan. (Anda dapat berlangganan beberapa antrian ke satu topik SNS.) Untuk informasi selengkapnya, lihat Mengirim Pesan Amazon SNS ke Antrian Amazon SQS.

Izin untuk Amazon SQS

Untuk menggunakan Amazon SQS AWS Config, Anda harus mengonfigurasi kebijakan yang memberikan izin ke akun Anda untuk melakukan semua tindakan yang diizinkan pada antrean SQS. Contoh kebijakan berikut memberikan izin nomor akun 111122223333 dan nomor akun

444455556666 untuk mengirim pesan yang berkaitan dengan setiap perubahan konfigurasi ke antrian bernama arn:aws:sqs:us-east- 2:444455556666:queue1.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "Queue1_Policy_UUID",
  "Statement":
    {
       "Sid":"Queue1_SendMessage",
       "Effect": "Allow",
       "Principal": {
            "AWS": ["111122223333","444455556666"]
         },
        "Action": "sqs:SendMessage",
        "Resource": "arn:aws:sqs:us-east-2:444455556666:queue1"
     }
}
```

Anda juga harus membuat kebijakan yang memberikan izin untuk koneksi antara topik SNS dan antrean SQS yang berlangganan topik tersebut. Berikut ini adalah contoh kebijakan yang mengizinkan topik SNS dengan Amazon Resource Name (ARN) arn:aws:sns:us-east-2:111122223333:test-topic untuk melakukan tindakan apa pun pada antrian bernama arn:aws:sqs:us-east- 2:111122223333:. test-topic-queue

> **Note**
>
> Akun untuk topik SNS dan antrian SQS harus berada di wilayah yang sama.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "SNStoSQS",
  "Statement":
    {
```

```
      "Sid":"rule1",
      "Effect": "Allow",
      "Principal": {
        "Service": "sns.amazonaws.com"
      },
      "Action": "SQS:SendMessage",
      "Resource": "arn:aws:sqs:us-east-2:111122223333:test-topic-queue",
      "Condition" : {
        "StringEquals" : {
          "aws:SourceArn":"arn:aws:sns:us-east-2:111122223333:test-topic"
        }
      }
    }
}
```

Setiap kebijakan dapat menyertakan pernyataan yang hanya mencakup satu antrian, bukan beberapa antrian. Untuk informasi tentang pembatasan lain pada kebijakan Amazon SQS, lihat Informasi Khusus untuk Kebijakan Amazon SQS.

Pemantauan AWS Config dengan Amazon EventBridge

Amazon EventBridge memberikan aliran peristiwa sistem yang mendekati real-time yang menggambarkan perubahan AWS sumber daya. Gunakan Amazon EventBridge untuk mendeteksi dan bereaksi terhadap perubahan status AWS Config peristiwa.

Anda dapat membuat aturan yang berjalan setiap kali terjadi status transisi, atau saat ada transisi ke satu atau beberapa status yang penting. Kemudian, berdasarkan aturan yang Anda buat, Amazon EventBridge memanggil satu atau beberapa tindakan target saat peristiwa cocok dengan nilai yang Anda tentukan dalam aturan. Bergantung pada jenis acara, Anda mungkin ingin mengirim pemberitahuan, menangkap informasi acara, mengambil tindakan korektif, memulai acara, atau mengambil tindakan lain.

Namun AWS Config, sebelum Anda membuat aturan acara, Anda harus melakukan hal berikut:

- Biasakan diri Anda dengan acara, aturan, dan target di EventBridge. Untuk informasi selengkapnya, lihat Apa itu Amazon EventBridge?
- Untuk informasi selengkapnya tentang cara memulai EventBridge dan menyiapkan aturan, lihat Memulai Amazon EventBridge.
- Buat target yang akan Anda gunakan dalam aturan kejadian Anda.

Topik

- Pertimbangan
- EventBridge Format Amazon untuk AWS Config
- Membuat EventBridge Aturan Amazon untuk AWS Config

Pertimbangan

Anda tidak akan menerima peringatan EventBridge untuk jenis sumber daya berikut jika Anda tidak merekamnya dengan AWS Config:

- `AWS::ACM::Certificate`
- `AWS::CloudTrail::Trail`
- `AWS::CloudWatch::Alarm`
- `AWS::EC2::CustomerGateway`
- `AWS::EC2::EIP`
- `AWS::EC2::Host`
- `AWS::EC2::Instance`
- `AWS::EC2::InternetGateway`
- `AWS::EC2::NetworkAcl`
- `AWS::EC2::NetworkInterface`
- `AWS::EC2::RouteTable`
- `AWS::EC2::SecurityGroup`
- `AWS::EC2::Subnet`
- `AWS::EC2::VPC`
- `AWS::EC2::VPNConnection`
- `AWS::EC2::VPNGateway`
- `AWS::EC2::Volume`
- `AWS::ElasticLoadBalancingV2::LoadBalancer`
- `AWS::IAM::Group`
- `AWS::IAM::Policy`

- AWS::IAM::Role
- AWS::IAM::User
- AWS::RDS::DBInstance
- AWS::RDS::DBSecurityGroup
- AWS::RDS::DBSnapshot
- AWS::RDS::DBSubnetGroup
- AWS::RDS::EventSubscription
- AWS::Redshift::Cluster
- AWS::Redshift::ClusterParameterGroup
- AWS::Redshift::ClusterSecurityGroup
- AWS::Redshift::ClusterSnapshot
- AWS::Redshift::ClusterSubnetGroup
- AWS::Redshift::EventSubscription
- AWS::S3::Bucket

EventBridge Format Amazon untuk AWS Config

EventBridge Acara untuk AWS Config memiliki format sebagai berikut:

```
{
   "version": "0",
   "id": "cd4d811e-ab12-322b-8255-872ce65b1bc8",
   "detail-type": "event type",
   "source": "aws.config",
   "account": "111122223333",
   "time": "2018-03-22T00:38:11Z",
   "region": "us-east-1",
   "resources": [
      resources
   ],
   "detail": {
      specific message type
   }
}
```

Membuat EventBridge Aturan Amazon untuk AWS Config

Gunakan langkah-langkah berikut untuk membuat EventBridge aturan yang memicu peristiwa yang dipancarkan oleh. AWS Config Peristiwa dipancarkan atas dasar upaya terbaik.

1. Di panel navigasi, pilih Aturan.
2. Pilih Buat aturan.
3. Masukkan nama dan deskripsi untuk aturan.

   Aturan tidak boleh memiliki nama yang sama dengan aturan lain di Wilayah yang sama dan di bus kejadian yang sama.

   > **Note**
   >
   > Bus acara menerima peristiwa dari sumber, menggunakan aturan untuk mengevaluasinya, menerapkan transformasi input yang dikonfigurasi, dan merutekkannya ke target yang sesuai. Bus acara default akun Anda menerima acara dari Layanan AWS. Bus acara khusus dapat menerima acara dari aplikasi dan layanan khusus Anda. Bus acara mitra menerima acara dari sumber acara yang dibuat oleh mitra SaaS. Peristiwa ini berasal dari layanan atau aplikasi mitra. Untuk informasi selengkapnya, lihat Bus acara EventBridge di Amazon di Panduan EventBridge Pengguna Amazon.

4. Untuk Tipe aturan, pilih Aturan dengan pola peristiwa.
5. Untuk sumber Acara, pilih AWS acara atau acara EventBridge mitra.
6. (Opsional) Untuk jenis acara Contoh, pilih AWS acara.
7. (Opsional) Untuk contoh peristiwa, pilih jenis acara yang memicu aturan:
   - Pilih AWS API Call dari CloudTrail ke aturan dasar pada panggilan API yang dilakukan ke layanan ini. Untuk informasi selengkapnya tentang membuat jenis aturan ini, lihat Tutorial: Membuat EventBridge aturan Amazon untuk panggilan AWS CloudTrail API.
   - Pilih Config Configuration Item Change untuk mendapatkan notifikasi saat sumber daya di akun Anda berubah.

     Seperti yang dijelaskan dalam artikel dukungan ini, Anda dapat menggunakan EventBridge untuk menerima pemberitahuan email kustom ketika sumber daya dibuat atau dihapus, Bagaimana saya bisa menerima pemberitahuan email kustom ketika sumber daya dibuat di

AWS Config layanan saya Akun AWS menggunakan? dan Bagaimana saya bisa menerima pemberitahuan email khusus ketika sumber daya dihapus di AWS Config layanan yang saya Akun AWS gunakan? .

- Pilih Perubahan Kepatuhan Aturan Konfigurasi untuk mendapatkan pemberitahuan saat pemeriksaan kepatuhan terhadap aturan Anda gagal.

  Seperti yang dijelaskan dalam artikel dukungan ini, Anda dapat menggunakan EventBridge untuk menerima pemberitahuan email khusus ketika sumber daya tidak sesuai, Bagaimana saya bisa diberi tahu ketika AWS sumber daya tidak sesuai menggunakan? AWS Config .
- Pilih Status Evaluasi Ulang Aturan Config untuk mendapatkan notifikasi status evaluasi ulang.
- Pilih Status Pengiriman Snapshot Konfigurasi Konfigurasi Konfigurasi untuk mendapatkan pemberitahuan status pengiriman snapshot konfigurasi.
- Pilih Status Pengiriman Riwayat Konfigurasi Konfigurasi Konfigurasi untuk mendapatkan pemberitahuan status pengiriman riwayat konfigurasi.

8. Untuk metode Creation, pilih Gunakan formulir pola.
9. Untuk Sumber peristiwa, pilih Layanan AWS .
10. Untuk AWS layanan, pilih Config.
11. Untuk jenis Acara, pilih jenis acara yang memicu aturan:
    - Pilih Semua Acara untuk membuat aturan yang berlaku untuk semua AWS layanan. Jika memilih opsi ini, Anda tidak dapat memilih jenis pesan tertentu, nama aturan, jenis sumber daya, atau sumber daya IDs.
    - Pilih AWS API Call dari CloudTrail ke aturan dasar pada panggilan API yang dilakukan ke layanan ini. Untuk informasi selengkapnya tentang membuat jenis aturan ini, lihat Tutorial: Membuat EventBridge aturan Amazon untuk panggilan AWS CloudTrail API.
    - Pilih Config Configuration Item Change untuk mendapatkan notifikasi saat sumber daya di akun Anda berubah.

      Seperti yang dijelaskan dalam artikel dukungan ini, Anda dapat menggunakan EventBridge untuk menerima pemberitahuan email kustom ketika sumber daya dibuat atau dihapus, Bagaimana saya bisa menerima pemberitahuan email kustom ketika sumber daya dibuat di AWS Config layanan saya Akun AWS menggunakan? dan Bagaimana saya bisa menerima pemberitahuan email khusus ketika sumber daya dihapus di AWS Config layanan yang saya Akun AWS gunakan? .
    - Pilih Perubahan Kepatuhan Aturan Konfigurasi untuk mendapatkan pemberitahuan saat pemeriksaan kepatuhan terhadap aturan Anda gagal.

Seperti yang dijelaskan dalam artikel dukungan ini, Anda dapat menggunakan EventBridge untuk menerima pemberitahuan email khusus ketika sumber daya tidak sesuai, Bagaimana saya bisa diberi tahu ketika AWS sumber daya tidak sesuai menggunakan? AWS Config .

- Pilih Status Evaluasi Ulang Aturan Config untuk mendapatkan notifikasi status evaluasi ulang.
- Pilih Status Pengiriman Snapshot Konfigurasi Konfigurasi Konfigurasi untuk mendapatkan pemberitahuan status pengiriman snapshot konfigurasi.
- Pilih Status Pengiriman Riwayat Konfigurasi Konfigurasi Konfigurasi untuk mendapatkan pemberitahuan status pengiriman riwayat konfigurasi.

12. Pilih Jenis pesan apa pun untuk menerima pemberitahuan jenis apa pun. Pilih Jenis pesan tertentu untuk menerima jenis pemberitahuan berikut:
    - Jika Anda memilih ConfigurationItemChangeNotification, Anda menerima pesan ketika konfigurasi sumber daya yang AWS Config mengevaluasi telah berubah.
    - Jika Anda memilih ComplianceChangeNotification, Anda menerima pesan ketika jenis kepatuhan sumber daya yang AWS Config mengevaluasi telah berubah.
    - Jika Anda memilih ConfigRulesEvaluationStarted, Anda menerima pesan saat AWS Config mulai mengevaluasi aturan Anda terhadap sumber daya yang ditentukan.
    - Jika mau ConfigurationSnapshotDeliveryCompleted, Anda akan menerima pesan saat AWS Config berhasil mengirimkan snapshot konfigurasi ke bucket Amazon S3 Anda.
    - Jika mau ConfigurationSnapshotDeliveryFailed, Anda akan menerima pesan saat AWS Config gagal mengirimkan snapshot konfigurasi ke bucket Amazon S3 Anda.
    - Jika mau ConfigurationSnapshotDeliveryStarted, Anda akan menerima pesan saat AWS Config mulai mengirimkan snapshot konfigurasi ke bucket Amazon S3 Anda.
    - Jika mau ConfigurationHistoryDeliveryCompleted, Anda menerima pesan saat AWS Config berhasil mengirimkan riwayat konfigurasi ke bucket Amazon S3 Anda.
13. Jika Anda memilih jenis peristiwa tertentu dari daftar tarik-turun Jenis Peristiwa, pilih Jenis sumber daya apa pun untuk membuat aturan yang berlaku untuk semua jenis sumber daya yang AWS Config didukung.

    Atau pilih Jenis sumber daya tertentu, lalu ketik jenis sumber daya yang AWS Config didukung (misalnya,`AWS::EC2::Instance`).
14. Jika Anda memilih jenis peristiwa tertentu dari daftar tarik-turun Jenis Peristiwa, pilih ID sumber daya apa pun untuk menyertakan ID sumber daya yang AWS Config didukung.

Atau pilih ID sumber daya tertentu, lalu ketik ID sumber daya yang AWS Config didukung (misalnya,`i-04606de676e635647`).

15. Jika Anda memilih jenis peristiwa tertentu dari daftar tarik-turun Jenis Acara, pilih Nama aturan apa pun untuk menyertakan aturan yang AWS Config didukung.

    Atau pilih Nama aturan khusus, lalu ketik aturan yang AWS Config didukung (misalnya, tag yang diperlukan).

16. Untuk Pilih target, pilih jenis target yang telah Anda siapkan untuk digunakan dengan aturan ini, lalu konfigurasikan opsi tambahan apa pun yang diperlukan oleh jenis tersebut.
17. Bidang yang ditampilkan bervariasi tergantung pada layanan yang Anda pilih. Masukkan informasi khusus untuk jenis target ini sesuai kebutuhan.
18. Untuk banyak jenis target, EventBridge perlu izin untuk mengirim acara ke target. Dalam kasus ini, EventBridge dapat membuat peran IAM yang diperlukan agar aturan Anda berjalan.
    - Untuk membuat IAM role secara otomatis, pilih Buat peran baru untuk sumber daya khusus ini.
    - Untuk menggunakan IAM role yang Anda buat sebelumnya, pilih Gunakan peran yang ada.
19. (Opsional) Pilih Tambahkan target untuk menambahkan target lain untuk aturan ini.
20. (Opsional) Masukkan satu atau lebih tanda untuk aturan. Untuk informasi selengkapnya, lihat EventBridge Tag Amazon.
21. Tinjau pengaturan aturan Anda untuk memastikannya memenuhi persyaratan pemantauan kejadian Anda.
22. Pilih Buat untuk mengonfirmasi pilihan Anda.

Menggunakan AWS Config dengan Antarmuka Amazon VPC Endpoints

Jika Anda menggunakan Amazon Virtual Private Cloud (Amazon VPC) untuk meng-host AWS sumber daya Anda, Anda dapat membuat koneksi pribadi antara VPC dan VPC. AWS Config Anda dapat menggunakan koneksi ini untuk berkomunikasi AWS Config dari VPC Anda tanpa melalui internet publik.

Amazon VPC adalah AWS layanan yang dapat Anda gunakan untuk meluncurkan AWS sumber daya di jaringan virtual yang Anda tentukan. Dengan VPC, Anda memiliki kendali terhadap pengaturan jaringan, seperti rentang alamat IP, subnet, tabel rute, dan pintu masuk jaringan. Endpoint VPC antarmuka didukung oleh AWS PrivateLink, sebuah AWS teknologi yang memungkinkan komunikasi pribadi antara AWS layanan menggunakan antarmuka jaringan elastis dengan alamat IP pribadi. Untuk menghubungkan VPC Anda AWS Config, Anda menentukan titik akhir VPC antarmuka untuk. AWS Config Jenis titik akhir ini memungkinkan Anda untuk menghubungkan VPC AWS Anda ke layanan. Endpoint menyediakan konektivitas yang andal dan dapat diskalakan AWS Config tanpa memerlukan gateway internet, instance terjemahan alamat jaringan (NAT), atau koneksi VPN. Untuk informasi selengkapnya, lihat Apa yang dimaksud dengan Amazon VPC dalam Panduan Pengguna Amazon VPC.

Langkah-langkah berikut ditujukan untuk para pengguna Amazon VPC. Untuk informasi selengkapnya, silakan lihat Getting Started di Panduan Pengguna Amazon VPC.

Buat Endpoint VPC untuk AWS Config

Untuk mulai menggunakan AWS Config dengan VPC Anda, buat antarmuka VPC endpoint untuk. AWS Config Anda tidak perlu mengubah pengaturan untuk AWS Config. AWS Config memanggil AWS layanan lain menggunakan titik akhir publik mereka. Untuk informasi selengkapnya, lihat Pembuatan Titik Akhir Antarmuka dalam Panduan Pengguna Amazon VPC.

Pertanyaan yang Sering Diajukan

Tidak dapat melihat perubahan konfigurasi terbaru saya

Dapatkah saya berharap untuk melihat perubahan konfigurasi saya segera?

AWS Config biasanya mencatat perubahan konfigurasi ke sumber daya Anda tepat setelah perubahan terdeteksi, atau pada frekuensi yang Anda tentukan. Namun, ini atas dasar upaya terbaik dan kadang-kadang bisa memakan waktu lebih lama. Jika masalah berlanjut setelah beberapa waktu, hubungi Dukungandan berikan AWS Config metrik Anda yang didukung oleh Amazon. CloudWatch Untuk informasi tentang metrik ini, lihat Metrik AWS Config Penggunaan dan Sukses.

Hubungan Tidak Langsung di AWS Config

Topik

- Apa itu hubungan sumber daya?
- Apa hubungan langsung dan tidak langsung sehubungan dengan sumber daya?
- Hubungan tidak langsung mana yang AWS Config mendukung?
- Skenario mana yang menggunakan hubungan tidak langsung?
- Bagaimana item konfigurasi dibuat karena hubungan langsung dan tidak langsung?
- Apa item konfigurasi yang dihasilkan karena hubungan tidak langsung?
- Bagaimana cara menonaktifkan hubungan tidak langsung?
- Bagaimana cara mengambil data konfigurasi yang terkait dengan hubungan tidak langsung?

Apa itu hubungan sumber daya?

Di AWS, sumber daya merujuk ke entitas yang dapat dikelola, seperti instans Amazon Elastic Compute Cloud EC2 (Amazon), AWS CloudFormation tumpukan, atau bucket Amazon S3. AWS Config adalah layanan yang melacak dan memantau sumber daya dengan membuat item konfigurasi (CIs) setiap kali perubahan ke jenis sumber daya yang direkam terdeteksi, atau pada frekuensi perekaman yang Anda tetapkan. Misalnya, ketika AWS Config diatur untuk melacak EC2 instans Amazon, itu akan membuat item konfigurasi setiap kali instance dibuat, diperbarui,

atau dihapus. Setiap item konfigurasi yang dibuat oleh AWS Config memiliki beberapa bidang, termasuk`accountId`, `arn` (Nama Sumber Daya Amazon),`awsRegion`,`configuration`,`tags`, dan`relationships`. Bidang hubungan CI memungkinkan AWS Config untuk menampilkan bagaimana sumber daya dihubungkan satu sama lain. Misalnya, hubungan dapat menunjukkan bahwa volume Amazon EBS dengan ID `vol-123ab45d` dilampirkan ke EC2 instans Amazon dengan ID`i-a1b2c3d4`, yang terkait dengan grup `sg-ef678hk` keamanan.

Apa hubungan langsung dan tidak langsung sehubungan dengan sumber daya?

AWS Config menurunkan hubungan untuk sebagian besar jenis sumber daya dari bidang konfigurasi, yang disebut hubungan “langsung”. Hubungan langsung adalah koneksi satu arah (A→B) antara sumber daya (A) dan sumber daya lain (B), biasanya diperoleh dari respon API deskripsi sumber daya (A). Di masa lalu, untuk beberapa jenis sumber daya yang AWS Config awalnya didukung, ia juga menangkap hubungan dari konfigurasi sumber daya lain, menciptakan hubungan “tidak langsung” yang dua arah (B→A). Misalnya, hubungan antara EC2 instans Amazon dan grup keamanannya bersifat langsung karena grup keamanan disertakan dalam respons API deskripsi untuk EC2 instans Amazon. Di sisi lain, hubungan antara grup keamanan dan EC2 instans Amazon tidak langsung karena menggambarkan grup keamanan tidak mengembalikan informasi apa pun tentang instance yang terkait dengannya.

Misalnya, hubungan tidak langsung dapat membantu menjawab pertanyaan-pertanyaan berikut:

- Ketika Gateway NAT gagal, EC2 instance mana di subnet pribadi yang terpengaruh?
- Jika tabel rute dimodifikasi, EC2 instance mana yang mungkin mengalami masalah konektivitas?
- Kelompok keamanan mana yang tidak pernah digunakan?
- ENI sekunder mana yang melekat pada EC2 instance yang terkait dengan grup keamanan?

Akibatnya, ketika perubahan konfigurasi sumber daya terdeteksi, AWS Config tidak hanya membuat CI untuk sumber daya itu, tetapi juga menghasilkan CIs untuk sumber daya terkait, termasuk yang memiliki hubungan tidak langsung. Misalnya, ketika AWS Config mendeteksi perubahan dalam EC2 instans Amazon, itu membuat CI untuk instance dan CI untuk grup keamanan yang terkait dengan instance.

Hubungan tidak langsung mana yang AWS Config mendukung?

Hubungan sumber daya tidak langsung berikut didukung di AWS Config.

Jenis sumber daya	secara tidak langsung terkait dengan jenis sumber daya		
AWS::EC2::RouteTable	AWS::EC2::Instance , AWS::EC2::NetworkInterface , AWS::EC2::Subnet , AWS::EC2::VPNGateway , AWS::EC2::VPC		
AWS::EC2::EIP	AWS::EC2::Instance , AWS::EC2::NetworkInterface		
AWS::EC2::Instance	AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkInterface	AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkACL	AWS::EC2::Subnet , AWS::EC2::VPC		

Jenis sumber daya	secara tidak langsung terkait dengan jenis sumber daya		
`AWS::EC2::VPNConnection`	`AWS::EC2::VPNGateway` , `AWS::EC2::CustomerGateway`		
`AWS::EC2::InternetGateway`	`AWS::EC2::VPC`		
`AWS::EC2::SecurityGroup`	`AWS::EC2::VPC`		
`AWS::EC2::Subnet`	`AWS::EC2::VPC`		
`AWS::EC2::VPNGateway`	`AWS::EC2::VPC`		

Skenario mana yang menggunakan hubungan tidak langsung?

Di bawah ini adalah AWS layanan dan fitur layanan menggunakan hubungan tidak langsung.

AWS fitur	Skenario
AWS Config aturan terkelola	Aturan ec2- security-group-attached-to -eni memeriksa apakah grup keamanan non-defau lt dilampirkan ke Antarmuka Jaringan Elastis (ENI). Tanpa hubungan tidak langsung, Anda perlu membuat aturan khusus untuk memeriksa

AWS fitur	Skenario
	apakah grup keamanan non-default dilampirkan ke ENI.
AWS Firewall Manager	Kebijakan Grup Keamanan Audit Penggunaan menggunakan hubungan tidak langsung untuk memahami kapan grup keamanan terakhir digunakan. Tanpa hubungan tidak langsung, Anda perlu membangun dan mengaitkan grup keamanan dengan sumber daya baru pada saat yang sama untuk menghindari memicu aturan dengan AWS Firewall Manager.

Sumber daya default	• Sumber daya default saat VPC non-default dibuat:
	  • Grup keamanan default, ACL jaringan default, dan tabel rute default.
	• Sumber daya default saat VPC default dibuat:
	  • Segala sesuatu yang dibuat dengan VPC non-default, gateway internet, dan subnet default di setiap Availability Zone yang dapat Anda akses.
	• Pembuatan VPC default itu sendiri saat akun menelepon EC2 untuk pertama kalinya.
	  • Subnet default dibuat untuk akun di Availability Zone yang baru diluncurkan.
	
	Tanpa hubungan tidak langsung, Anda harus menunggu hingga 12 jam agar anti-entropi merekam perubahan pada sumber daya default.

Bagaimana item konfigurasi dibuat karena hubungan langsung dan tidak langsung?

Untuk hubungan langsung antara sumber daya (A→B), setiap perubahan konfigurasi ke sumber daya B akan memulai item konfigurasi (CI) untuk sumber daya A juga. Demikian pula, untuk hubungan tidak langsung (B → A), ketika ada perubahan konfigurasi ke sumber daya A CI baru akan dihasilkan untuk sumber daya B. EC2 Misalnya, instans Amazon ke grup keamanan adalah hubungan langsung sehingga setiap perubahan konfigurasi ke grup keamanan akan menghasilkan CI untuk grup keamanan serta CI untuk instance. EC2 Demikian pula, grup keamanan ke EC2 instans Amazon adalah hubungan tidak langsung sehingga setiap perubahan konfigurasi ke EC2 instance akan menghasilkan CI untuk EC2 instans Amazon serta CI untuk grup keamanan.

Apa item konfigurasi yang dihasilkan karena hubungan tidak langsung?

Di bawah ini adalah item konfigurasi tambahan (CIs) yang dihasilkan karena hubungan sumber daya tidak langsung.

Perubahan konfigurasi ke jenis sumber daya berikut	akan menghasilkan CIs untuk jenis sumber daya berikut		
`AWS::EC2::RouteTable`	`AWS::EC2::Instance` ,`AWS::EC2::NetworkInterface` ,`AWS::EC2::Subnet` ,`AWS::EC2::VPNGateway` , dan `AWS::EC2::VPC`		
`AWS::EC2::EIP`	`AWS::EC2::Instance` , `AWS::EC2::NetworkInterface`		

Perubahan konfigurasi ke jenis sumber daya berikut	akan menghasilkan CIs untuk jenis sumber daya berikut		
AWS::EC2::Instance	AWS::EC2::Security Group , AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkInterface	AWS::EC2::Security Group , AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkACL	AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::VPNConnection	AWS::EC2::VPNGateway , AWS::EC2::Customer Gateway		
AWS::EC2::Internet Gateway	AWS::EC2::VPC		
AWS::EC2::SecurityGroup	AWS::EC2::VPC		
AWS::EC2::Subnet	AWS::EC2::VPC		
AWS::EC2::VPNGateway	AWS::EC2::VPC		

Bagaimana cara menonaktifkan hubungan tidak langsung?

Selesaikan langkah-langkah berikut untuk menonaktifkan hubungan tidak langsung:

1. Buka AWS Dukungan kasing dari akun Anda atau dari akun manajemen untuk beberapa akun.
2. Pilih Teknis untuk jenis dukungan.
3. Untuk Layanan, pilih AWS Config.
4. Untuk Kategori, pilih Lainnya.
5. Pilih tingkat keparahan yang sesuai.
6. Masukkan Nonaktifkan Hubungan Tidak Langsung di baris subjek.
7. Dalam deskripsi:
   - Konfirmasikan bahwa Anda telah membaca FAQ ini dan ingin melanjutkan.
   - Buat daftar wilayah tempat Anda ingin menonaktifkan hubungan tidak langsung.
   - Jika mengirimkan dari akun manajemen, sertakan akun IDs dan wilayah terkait mereka.
   - Untuk beberapa akun, Anda dapat melampirkan file CSV dengan akun IDs dan wilayah.

Seorang AWS Dukungan insinyur akan memberikan langkah selanjutnya dan pembaruan status. Kami menyarankan Anda mempertahankan daftar AWS akun dan wilayah di mana hubungan tidak langsung dinonaktifkan. Untuk akun baru, kirimkan AWS Dukungan kasus baru untuk menonaktifkan hubungan tidak langsung.

Bagaimana cara mengambil data konfigurasi yang terkait dengan hubungan tidak langsung?

Anda dapat menjalankan kueri Structured Query Language (SQL) di Kueri AWS Config Lanjutan untuk mengambil data konfigurasi yang terkait dengan hubungan sumber daya tidak langsung. Misalnya, jika Anda ingin mengambil daftar EC2 instans Amazon yang terkait dengan grup keamanan, gunakan kueri berikut:

```
SELECT
    resourceId,
    resourceType
    WHERE
    resourceType ='AWS::EC2::Instance'
    AND
    relationships.resourceId = 'sg-234213'
```

Contoh kode untuk AWS Config menggunakan AWS SDKs

Contoh kode berikut menunjukkan cara menggunakan AWS Config kit pengembangan AWS perangkat lunak (SDK).

Tindakan merupakan kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Sementara tindakan menunjukkan cara memanggil fungsi layanan individual, Anda dapat melihat tindakan dalam konteks dalam skenario terkait.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Config dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Contoh kode

- Contoh dasar untuk AWS Config menggunakan AWS SDKs
  - Tindakan untuk AWS Config menggunakan AWS SDKs
    - Gunakan DeleteConfigRule dengan AWS SDK atau CLI
    - Gunakan DescribeComplianceByConfigRule dengan CLI
    - Gunakan DescribeComplianceByResource dengan CLI
    - Gunakan DescribeConfigRuleEvaluationStatus dengan CLI
    - Gunakan DescribeConfigRules dengan AWS SDK atau CLI
    - Gunakan DescribeConfigurationRecorderStatus dengan CLI
    - Gunakan DescribeConfigurationRecorders dengan CLI
    - Gunakan DescribeDeliveryChannels dengan CLI
    - Gunakan GetComplianceDetailsByConfigRule dengan CLI
    - Gunakan GetComplianceDetailsByResource dengan CLI
    - Gunakan GetComplianceSummaryByConfigRule dengan CLI
    - Gunakan GetComplianceSummaryByResourceType dengan CLI
    - Gunakan PutConfigRule dengan AWS SDK atau CLI
    - Gunakan PutDeliveryChannel dengan CLI

Contoh dasar untuk AWS Config menggunakan AWS SDKs

Contoh kode berikut menunjukkan cara menggunakan dasar-dasar AWS Config dengan AWS SDKs.

Contoh

- Tindakan untuk AWS Config menggunakan AWS SDKs
  - Gunakan DeleteConfigRule dengan AWS SDK atau CLI
  - Gunakan DescribeComplianceByConfigRule dengan CLI
  - Gunakan DescribeComplianceByResource dengan CLI
  - Gunakan DescribeConfigRuleEvaluationStatus dengan CLI
  - Gunakan DescribeConfigRules dengan AWS SDK atau CLI
  - Gunakan DescribeConfigurationRecorderStatus dengan CLI
  - Gunakan DescribeConfigurationRecorders dengan CLI
  - Gunakan DescribeDeliveryChannels dengan CLI
  - Gunakan GetComplianceDetailsByConfigRule dengan CLI
  - Gunakan GetComplianceDetailsByResource dengan CLI
  - Gunakan GetComplianceSummaryByConfigRule dengan CLI
  - Gunakan GetComplianceSummaryByResourceType dengan CLI
  - Gunakan PutConfigRule dengan AWS SDK atau CLI
  - Gunakan PutDeliveryChannel dengan CLI

Tindakan untuk AWS Config menggunakan AWS SDKs

Contoh kode berikut menunjukkan bagaimana melakukan AWS Config tindakan individu dengan AWS SDKs. Setiap contoh menyertakan tautan ke GitHub, di mana Anda dapat menemukan instruksi untuk mengatur dan menjalankan kode.

Contoh berikut hanya mencakup tindakan yang paling umum digunakan. Untuk daftar lengkapnya, lihat Referensi AWS Config API.

Contoh

- Gunakan DeleteConfigRule dengan AWS SDK atau CLI
- Gunakan DescribeComplianceByConfigRule dengan CLI
- Gunakan DescribeComplianceByResource dengan CLI
- Gunakan DescribeConfigRuleEvaluationStatus dengan CLI
- Gunakan DescribeConfigRules dengan AWS SDK atau CLI
- Gunakan DescribeConfigurationRecorderStatus dengan CLI

- Gunakan DescribeConfigurationRecorders dengan CLI
- Gunakan DescribeDeliveryChannels dengan CLI
- Gunakan GetComplianceDetailsByConfigRule dengan CLI
- Gunakan GetComplianceDetailsByResource dengan CLI
- Gunakan GetComplianceSummaryByConfigRule dengan CLI
- Gunakan GetComplianceSummaryByResourceType dengan CLI
- Gunakan PutConfigRule dengan AWS SDK atau CLI
- Gunakan PutDeliveryChannel dengan CLI

Gunakan **`DeleteConfigRule`** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan`DeleteConfigRule`.

CLI

AWS CLI

Untuk menghapus aturan AWS Config

Perintah berikut menghapus aturan AWS Config bernama: `MyConfigRule`

```
aws configservice delete-config-rule --config-rule-name MyConfigRule
```

- Untuk detail API, lihat DeleteConfigRuledi Referensi AWS CLI Perintah.

Python

SDK untuk Python (Boto3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

```
class ConfigWrapper:
```

```
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def delete_config_rule(self, rule_name):
        """
        Delete the specified rule.

        :param rule_name: The name of the rule to delete.
        """
        try:
            self.config_client.delete_config_rule(ConfigRuleName=rule_name)
            logger.info("Deleted rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't delete rule %s.", rule_name)
            raise
```

- Untuk detail API, lihat DeleteConfigRuledi AWS SDK for Python (Boto3) Referensi API.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Config dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **`DescribeComplianceByConfigRule`** dengan CLI

Contoh kode berikut menunjukkan cara menggunakan`DescribeComplianceByConfigRule`.

CLI

AWS CLI

Untuk mendapatkan informasi kepatuhan untuk aturan AWS Config Anda

Perintah berikut menampilkan informasi kepatuhan untuk setiap aturan AWS Config yang dilanggar oleh satu atau beberapa sumber daya: AWS

```
aws configservice describe-compliance-by-config-rule --compliance-
types NON_COMPLIANT
```

Dalam output, nilai untuk setiap `CappedCount` atribut menunjukkan berapa banyak sumber daya yang tidak sesuai dengan aturan terkait. Misalnya, output berikut menunjukkan bahwa 3 sumber daya tidak sesuai dengan aturan bernama`InstanceTypesAreT2micro`.

Output:

```
{
    "ComplianceByConfigRules": [
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "InstanceTypesAreT2micro"
        },
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "RequiredTagsForVolumes"
        }
    ]
}
```

- Untuk detail API, lihat DescribeComplianceByConfigRuledi Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Contoh ini mengambil rincian kepatuhan untuk aturan ebs-optimized-instance, yang tidak ada hasil evaluasi saat ini untuk aturan, sehingga mengembalikan INSUFFICIENT_DATA

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

Output:

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

Contoh 2: Contoh ini mengembalikan jumlah sumber daya yang tidak sesuai untuk aturan ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK.

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

Output:

```
CapExceeded CappedCount
----------- -----------
False       2
```

- Untuk detail API, lihat DescribeComplianceByConfigRuledi Referensi Alat AWS untuk PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Contoh ini mengambil rincian kepatuhan untuk aturan ebs-optimized-instance, yang tidak ada hasil evaluasi saat ini untuk aturan, sehingga mengembalikan INSUFFICIENT_DATA

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

Output:

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

Contoh 2: Contoh ini mengembalikan jumlah sumber daya yang tidak sesuai untuk aturan ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK.

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

Output:

```
CapExceeded CappedCount
----------- -----------
False       2
```

- Untuk detail API, lihat DescribeComplianceByConfigRuledi Referensi Alat AWS untuk PowerShell Cmdlet (V5).

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Config dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan `DescribeComplianceByResource` dengan CLI

Contoh kode berikut menunjukkan cara menggunakan`DescribeComplianceByResource`.

CLI

AWS CLI

Untuk mendapatkan informasi kepatuhan untuk AWS sumber daya Anda

Perintah berikut mengembalikan informasi kepatuhan untuk setiap EC2 instance yang direkam oleh AWS Config dan yang melanggar satu atau beberapa aturan:

```
aws configservice describe-compliance-by-resource --resource-
type AWS::EC2::Instance --compliance-types NON_COMPLIANT
```

Dalam output, nilai untuk setiap `CappedCount` atribut menunjukkan berapa banyak aturan yang dilanggar sumber daya. Misalnya, output berikut menunjukkan bahwa instance `i-1a2b3c4d` melanggar 2 aturan.

Output:

```
{
    "ComplianceByResources": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-1a2b3c4d",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 2,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-2a2b3c4d ",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        }
    ]
}
```

- Untuk detail API, lihat DescribeComplianceByResourcedi Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Contoh ini memeriksa jenis **`AWS::SSM::ManagedInstanceInventory`** sumber daya untuk jenis kepatuhan 'COMPLIANT'.

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

Output:

```
Compliance                            ResourceId          ResourceType
----------                            ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- Untuk detail API, lihat DescribeComplianceByResourcedi Referensi Alat AWS untuk PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Contoh ini memeriksa jenis **`AWS::SSM::ManagedInstanceInventory`** sumber daya untuk jenis kepatuhan 'COMPLIANT'.

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

Output:

```
Compliance                            ResourceId          ResourceType
----------                            ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- Untuk detail API, lihat DescribeComplianceByResourcedi Referensi Alat AWS untuk PowerShell Cmdlet (V5).

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Config dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **`DescribeConfigRuleEvaluationStatus`** dengan CLI

Contoh kode berikut menunjukkan cara menggunakan`DescribeConfigRuleEvaluationStatus`.

CLI

AWS CLI

Untuk mendapatkan informasi status untuk aturan AWS Config

Perintah berikut mengembalikan informasi status untuk aturan AWS Config bernama: `MyConfigRule`

```
aws configservice describe-config-rule-evaluation-status --config-rule-
names MyConfigRule
```

Output:

```
{
    "ConfigRulesEvaluationStatus": [
        {
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "FirstActivatedTime": 1450311703.844,
            "ConfigRuleId": "config-rule-abcdef",
            "LastSuccessfulInvocationTime": 1450314643.156,
            "ConfigRuleName": "MyConfigRule"
        }
    ]
}
```

- Untuk detail API, lihat DescribeConfigRuleEvaluationStatusdi Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Contoh ini mengembalikan informasi status untuk aturan konfigurasi yang diberikan.

```
Get-CFGConfigRuleEvaluationStatus -ConfigRuleName root-account-mfa-enabled, vpc-
flow-logs-enabled
```

Output:

```
ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-kvq1wk
ConfigRuleId                 : config-rule-kvq1wk
ConfigRuleName               : root-account-mfa-enabled
FirstActivatedTime           : 8/27/2019 8:05:17 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 8:12:03 AM
LastSuccessfulInvocationTime : 12/13/2019 8:12:03 AM

ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-z1s23b
ConfigRuleId                 : config-rule-z1s23b
ConfigRuleName               : vpc-flow-logs-enabled
FirstActivatedTime           : 8/14/2019 6:23:44 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 7:12:01 AM
LastSuccessfulInvocationTime : 12/13/2019 7:12:01 AM
```

- Untuk detail API, lihat DescribeConfigRuleEvaluationStatusdi Referensi Alat AWS untuk PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Contoh ini mengembalikan informasi status untuk aturan konfigurasi yang diberikan.

```
Get-CFGConfigRuleEvaluationStatus -ConfigRuleName root-account-mfa-enabled, vpc-
flow-logs-enabled
```

Output:

```
ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-kvq1wk
ConfigRuleId                 : config-rule-kvq1wk
```

```
ConfigRuleName               : root-account-mfa-enabled
FirstActivatedTime           : 8/27/2019 8:05:17 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 8:12:03 AM
LastSuccessfulInvocationTime : 12/13/2019 8:12:03 AM

ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-z1s23b
ConfigRuleId                 : config-rule-z1s23b
ConfigRuleName               : vpc-flow-logs-enabled
FirstActivatedTime           : 8/14/2019 6:23:44 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 7:12:01 AM
LastSuccessfulInvocationTime : 12/13/2019 7:12:01 AM
```

- Untuk detail API, lihat DescribeConfigRuleEvaluationStatusdi Referensi Alat AWS untuk PowerShell Cmdlet (V5).

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Config dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **`DescribeConfigRules`** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan`DescribeConfigRules`.

CLI

AWS CLI

Untuk mendapatkan detail tentang aturan AWS Config

Perintah berikut mengembalikan rincian untuk aturan AWS Config bernama: `InstanceTypesAreT2micro`

```
aws configservice describe-config-rules --config-rule-
names InstanceTypesAreT2micro
```

Output:

```
{
    "ConfigRules": [
        {
            "ConfigRuleState": "ACTIVE",
            "Description": "Evaluates whether EC2 instances are the t2.micro
 type.",
            "ConfigRuleName": "InstanceTypesAreT2micro",
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "Source": {
                "Owner": "CUSTOM_LAMBDA",
                "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
                "SourceDetails": [
                    {
                        "EventSource": "aws.config",
                        "MessageType": "ConfigurationItemChangeNotification"
                    }
                ]
            },
            "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}",
            "Scope": {
                "ComplianceResourceTypes": [
                    "AWS::EC2::Instance"
                ]
            },
            "ConfigRuleId": "config-rule-abcdef"
        }
    ]
}
```

- Untuk detail API, lihat DescribeConfigRulesdi Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Contoh ini mencantumkan aturan konfigurasi untuk akun, dengan properti yang dipilih.

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

Output:

```
ConfigRuleName                                     ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                     ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                              config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                                config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required         config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- Untuk detail API, lihat DescribeConfigRulesdi Referensi Alat AWS untuk PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Contoh ini mencantumkan aturan konfigurasi untuk akun, dengan properti yang dipilih.

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

Output:

```
ConfigRuleName                                    ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                    ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                             config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                               config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required        config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- Untuk detail API, lihat DescribeConfigRulesdi Referensi Alat AWS untuk PowerShell Cmdlet (V5).

Python

SDK untuk Python (Boto3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client
```

```
    def describe_config_rule(self, rule_name):
        """
        Gets data for the specified rule.

        :param rule_name: The name of the rule to retrieve.
        :return: The rule data.
        """
        try:
            response = self.config_client.describe_config_rules(
                ConfigRuleNames=[rule_name]
            )
            rule = response["ConfigRules"]
            logger.info("Got data for rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't get data for rule %s.", rule_name)
            raise
        else:
            return rule
```

- Untuk detail API, lihat DescribeConfigRulesdi AWS SDK for Python (Boto3) Referensi API.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Config dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **`DescribeConfigurationRecorderStatus`** dengan CLI

Contoh kode berikut menunjukkan cara menggunakan`DescribeConfigurationRecorderStatus`.

CLI

AWS CLI

Untuk mendapatkan informasi status untuk perekam konfigurasi

Perintah berikut mengembalikan status perekam konfigurasi default:

```
aws configservice describe-configuration-recorder-status
```

Output:

```
{
    "ConfigurationRecordersStatus": [
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "recording": true,
            "lastStatusChangeTime": 1452193834.344,
            "lastStartTime": 1441039997.819,
            "lastStopTime": 1441039992.835
        }
    ]
}
```

- Untuk detail API, lihat DescribeConfigurationRecorderStatusdi Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Sampel ini mengembalikan status perekam konfigurasi.

```
Get-CFGConfigurationRecorderStatus
```

Output:

```
LastErrorCode        :
LastErrorMessage     :
LastStartTime        : 10/11/2019 10:13:51 AM
LastStatus           : Success
LastStatusChangeTime : 12/31/2019 6:14:12 AM
LastStopTime         : 10/11/2019 10:13:46 AM
Name                 : default
Recording            : True
```

- Untuk detail API, lihat DescribeConfigurationRecorderStatusdi Referensi Alat AWS untuk PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Sampel ini mengembalikan status perekam konfigurasi.

```
Get-CFGConfigurationRecorderStatus
```

Output:

```
LastErrorCode        :
LastErrorMessage     :
LastStartTime        : 10/11/2019 10:13:51 AM
LastStatus           : Success
LastStatusChangeTime : 12/31/2019 6:14:12 AM
LastStopTime         : 10/11/2019 10:13:46 AM
Name                 : default
Recording            : True
```

- Untuk detail API, lihat DescribeConfigurationRecorderStatusdi Referensi Alat AWS untuk PowerShell Cmdlet (V5).

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Config dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **`DescribeConfigurationRecorders`** dengan CLI

Contoh kode berikut menunjukkan cara menggunakan`DescribeConfigurationRecorders`.

CLI

AWS CLI

Untuk mendapatkan detail tentang perekam konfigurasi

Perintah berikut mengembalikan rincian tentang perekam konfigurasi default:

```
aws configservice describe-configuration-recorders
```

Output:

```
{
    "ConfigurationRecorders": [
        {
            "recordingGroup": {
                "allSupported": true,
```

```
                "resourceTypes": [],
                "includeGlobalResourceTypes": true
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-ConfigRole-
A1B2C3D4E5F6",
            "name": "default"
        }
    ]
}
```

- Untuk detail API, lihat DescribeConfigurationRecordersdi Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Contoh ini mengembalikan rincian perekam konfigurasi.

```
Get-CFGConfigurationRecorder | Format-List
```

Output:

```
Name           : default
RecordingGroup : Amazon.ConfigService.Model.RecordingGroup
RoleARN        : arn:aws:iam::123456789012:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig
```

- Untuk detail API, lihat DescribeConfigurationRecordersdi Referensi Alat AWS untuk PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Contoh ini mengembalikan rincian perekam konfigurasi.

```
Get-CFGConfigurationRecorder | Format-List
```

Output:

```
Name           : default
RecordingGroup : Amazon.ConfigService.Model.RecordingGroup
RoleARN        : arn:aws:iam::123456789012:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig
```

- Untuk detail API, lihat DescribeConfigurationRecordersdi Referensi Alat AWS untuk PowerShell Cmdlet (V5).

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Config dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan `DescribeDeliveryChannels` dengan CLI

Contoh kode berikut menunjukkan cara menggunakan`DescribeDeliveryChannels`.

CLI

AWS CLI

Untuk mendapatkan detail tentang saluran pengiriman

Perintah berikut mengembalikan rincian tentang saluran pengiriman:

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

Output:

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

- Untuk detail API, lihat DescribeDeliveryChannelsdi Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Contoh ini mengambil saluran pengiriman untuk wilayah tersebut dan menampilkan detailnya.

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

Output:

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

- Untuk detail API, lihat DescribeDeliveryChannelsdi Referensi Alat AWS untuk PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Contoh ini mengambil saluran pengiriman untuk wilayah tersebut dan menampilkan detailnya.

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

Output:

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

- Untuk detail API, lihat DescribeDeliveryChannelsdi Referensi Alat AWS untuk PowerShell Cmdlet (V5).

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Config dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **`GetComplianceDetailsByConfigRule`** dengan CLI

Contoh kode berikut menunjukkan cara menggunakan`GetComplianceDetailsByConfigRule`.

CLI

AWS CLI

Untuk mendapatkan hasil evaluasi untuk aturan AWS Config

Perintah berikut mengembalikan hasil evaluasi untuk semua sumber daya yang tidak sesuai dengan aturan AWS Config bernama: `InstanceTypesAreT2micro`

```
aws configservice get-compliance-details-by-config-rule --config-rule-
name InstanceTypesAreT2micro --compliance-types NON_COMPLIANT
```

Output:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-2a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.18,
            "ConfigRuleInvokedTime": 1450314642.902,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
```

```
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-3a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.346,
            "ConfigRuleInvokedTime": 1450314643.124,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- Untuk detail API, lihat GetComplianceDetailsByConfigRuledi Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Contoh ini memperoleh hasil evaluasi untuk aturan access-keys-rotated dan mengembalikan output yang dikelompokkan berdasarkan tipe kepatuhan

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

Output:

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

Contoh 2: Contoh ini menanyakan detail kepatuhan access-keys-rotated untuk aturan sumber daya COMPLIANT.

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

Output:

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- Untuk detail API, lihat GetComplianceDetailsByConfigRuledi Referensi Alat AWS untuk PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Contoh ini memperoleh hasil evaluasi untuk aturan access-keys-rotated dan mengembalikan output yang dikelompokkan berdasarkan tipe kepatuhan

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

Output:

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

Contoh 2: Contoh ini menanyakan detail kepatuhan access-keys-rotated untuk aturan sumber daya COMPLIANT.

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

Output:

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- Untuk detail API, lihat GetComplianceDetailsByConfigRuledi Referensi Alat AWS untuk PowerShell Cmdlet (V5).

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Config dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **`GetComplianceDetailsByResource`** dengan CLI

Contoh kode berikut menunjukkan cara menggunakan`GetComplianceDetailsByResource`.

CLI

AWS CLI

Untuk mendapatkan hasil evaluasi untuk sumber AWS daya

Perintah berikut mengembalikan hasil evaluasi untuk setiap aturan yang EC2 instans `i-1a2b3c4d` tidak mematuhi:

```
aws configservice get-compliance-details-by-resource --resource-
type AWS::EC2::Instance --resource-id i-1a2b3c4d --compliance-types NON_COMPLIANT
```

Output:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
```

```
            },
            "ResultRecordedTime": 1450314643.288,
            "ConfigRuleInvokedTime": 1450314643.034,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "RequiredTagForEC2Instances"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- Untuk detail API, lihat GetComplianceDetailsByResourcedi Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Contoh evaulasi ini menghasilkan sumber daya yang diberikan.

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

Output:

```
Annotation                 :
ComplianceType             : COMPLIANT
ConfigRuleInvokedTime      : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime         : 8/25/2019 11:34:56 PM
ResultToken                :
```

- Untuk detail API, lihat GetComplianceDetailsByResourcedi Referensi Alat AWS untuk PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Contoh evaulasi ini menghasilkan sumber daya yang diberikan.

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

Output:

```
Annotation                 :
ComplianceType             : COMPLIANT
ConfigRuleInvokedTime      : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime         : 8/25/2019 11:34:56 PM
ResultToken                :
```

- Untuk detail API, lihat GetComplianceDetailsByResourcedi Referensi Alat AWS untuk PowerShell Cmdlet (V5).

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Config dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **`GetComplianceSummaryByConfigRule`** dengan CLI

Contoh kode berikut menunjukkan cara menggunakan`GetComplianceSummaryByConfigRule`.

CLI

AWS CLI

Untuk mendapatkan ringkasan kepatuhan untuk aturan AWS Config Anda

Perintah berikut mengembalikan jumlah aturan yang sesuai dan nomor yang tidak sesuai:

```
aws configservice get-compliance-summary-by-config-rule
```

Dalam output, nilai untuk setiap `CappedCount` atribut menunjukkan berapa banyak aturan yang sesuai atau tidak sesuai.

Output:

```
{
    "ComplianceSummary": {
        "NonCompliantResourceCount": {
            "CappedCount": 3,
            "CapExceeded": false
        },
        "ComplianceSummaryTimestamp": 1452204131.493,
        "CompliantResourceCount": {
            "CappedCount": 2,
            "CapExceeded": false
        }
    }
}
```

- Untuk detail API, lihat GetComplianceSummaryByConfigRuledi Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Contoh ini mengembalikan jumlah aturan Config yang tidak sesuai.

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

Output:

```
CapExceeded CappedCount
----------- -----------
False       9
```

- Untuk detail API, lihat GetComplianceSummaryByConfigRuledi Referensi Alat AWS untuk PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Contoh ini mengembalikan jumlah aturan Config yang tidak sesuai.

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

Output:

```
CapExceeded CappedCount
----------- -----------
False       9
```

- Untuk detail API, lihat GetComplianceSummaryByConfigRuledi Referensi Alat AWS untuk PowerShell Cmdlet (V5).

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Config dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **`GetComplianceSummaryByResourceType`** dengan CLI

Contoh kode berikut menunjukkan cara menggunakan`GetComplianceSummaryByResourceType`.

CLI

AWS CLI

Untuk mendapatkan ringkasan kepatuhan untuk semua jenis sumber daya

Perintah berikut mengembalikan jumlah AWS sumber daya yang tidak sesuai dan nomor yang sesuai:

```
aws configservice get-compliance-summary-by-resource-type
```

Dalam output, nilai untuk setiap `CappedCount` atribut menunjukkan berapa banyak sumber daya yang sesuai atau tidak sesuai.

Output:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 16,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1453237464.543,
                "CompliantResourceCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

Untuk mendapatkan ringkasan kepatuhan untuk jenis sumber daya tertentu

Perintah berikut mengembalikan jumlah EC2 instance yang tidak sesuai dan nomor yang sesuai:

```
aws configservice get-compliance-summary-by-resource-type --resource-
types AWS::EC2::Instance
```

Dalam output, nilai untuk setiap `CappedCount` atribut menunjukkan berapa banyak sumber daya yang sesuai atau tidak sesuai.

Output:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1452204923.518,
                "CompliantResourceCount": {
```

```
                    "CappedCount": 7,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

- Untuk detail API, lihat GetComplianceSummaryByResourceTypedi Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Sampel ini mengembalikan jumlah sumber daya yang sesuai atau tidak sesuai dan mengubah output menjadi json.

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- Untuk detail API, lihat GetComplianceSummaryByResourceTypedi Referensi Alat AWS untuk PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Sampel ini mengembalikan jumlah sumber daya yang sesuai atau tidak sesuai dan mengubah output menjadi json.

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
```

```
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- Untuk detail API, lihat GetComplianceSummaryByResourceTypedi Referensi Alat AWS untuk PowerShell Cmdlet (V5).

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Config dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **`PutConfigRule`** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan`PutConfigRule`.

CLI

AWS CLI

Untuk menambahkan aturan Config AWS terkelola

Perintah berikut menyediakan kode JSON untuk menambahkan aturan Config AWS terkelola:

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.json`adalah file JSON yang berisi konfigurasi aturan:

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
```

```
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

Untuk `ComplianceResourceTypes` atribut, kode JSON ini membatasi cakupan sumber daya `AWS::EC2::Instance` tipe, jadi AWS Config EC2 hanya akan mengevaluasi instance terhadap aturan. Karena aturan adalah aturan terkelola, `Owner` atribut diatur ke`AWS`, dan `SourceIdentifier` atribut diatur ke pengidentifikasi aturan,`REQUIRED_TAGS`. Untuk `InputParameters` atribut, kunci tag yang dibutuhkan aturan, `CostCenter` dan`Owner`, ditentukan.

Jika perintah berhasil, AWS Config tidak mengembalikan output. Untuk memverifikasi konfigurasi aturan, jalankan describe-config-rules perintah, dan tentukan nama aturan.

Untuk menambahkan aturan Config terkelola pelanggan

Perintah berikut menyediakan kode JSON untuk menambahkan aturan Config terkelola pelanggan:

```
aws configservice put-config-rule --config-rule file:// InstanceTypesAreT2micro.json
```

`InstanceTypesAreT2micro.json`adalah file JSON yang berisi konfigurasi aturan:

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
```

```
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

Untuk `ComplianceResourceTypes` atribut, kode JSON ini membatasi cakupan sumber daya `AWS::EC2::Instance` tipe, jadi AWS Config EC2 hanya akan mengevaluasi instance terhadap aturan. Karena aturan ini adalah aturan yang dikelola pelanggan, `Owner` atribut disetel ke`CUSTOM_LAMBDA`, dan `SourceIdentifier` atribut disetel ke ARN dari fungsi Lambda AWS . `SourceDetails`Objek diperlukan. Parameter yang ditentukan untuk `InputParameters` atribut diteruskan ke fungsi AWS Lambda saat AWS Config memanggilnya untuk mengevaluasi sumber daya terhadap aturan.

Jika perintah berhasil, AWS Config tidak mengembalikan output. Untuk memverifikasi konfigurasi aturan, jalankan describe-config-rules perintah, dan tentukan nama aturan.

- Untuk detail API, lihat PutConfigRuledi Referensi AWS CLI Perintah.

Python

SDK untuk Python (Boto3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di Repositori Contoh Kode AWS.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
```

```
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- Untuk detail API, lihat PutConfigRuledi AWS SDK for Python (Boto3) Referensi API.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Config dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **`PutDeliveryChannel`** dengan CLI

Contoh kode berikut menunjukkan cara menggunakan`PutDeliveryChannel`.

CLI

AWS CLI

Untuk membuat saluran pengiriman

Perintah berikut menyediakan pengaturan untuk saluran pengiriman sebagai kode JSON:

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

`deliveryChannel.json`File menentukan atribut saluran pengiriman:

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

Contoh ini menetapkan atribut berikut:

`name`- Nama saluran pengiriman. Secara default, AWS Config menetapkan nama `default` ke saluran pengiriman baru. Anda tidak dapat memperbarui nama saluran pengiriman dengan perintah. `put-delivery-channel` Untuk langkah-langkah mengubah nama, lihat Mengganti nama Saluran Pengiriman. `s3BucketName` - Nama bucket Amazon S3 tempat AWS Config memberikan snapshot konfigurasi dan file riwayat konfigurasi. Jika Anda menentukan bucket milik AWS akun lain, bucket tersebut harus memiliki kebijakan yang memberikan izin akses ke Config. AWS Untuk informasi selengkapnya, lihat Izin untuk Bucket Amazon S3.

`snsTopicARN`- Nama Sumber Daya Amazon (ARN) dari topik Amazon SNS tempat AWS Config mengirimkan pemberitahuan tentang perubahan konfigurasi. Jika Anda memilih topik dari akun lain, topik tersebut harus memiliki kebijakan yang memberikan izin akses ke Config. AWS Untuk informasi selengkapnya, lihat Izin untuk Topik Amazon SNS.

`configSnapshotDeliveryProperties`- Berisi `deliveryFrequency` atribut, yang menetapkan seberapa sering AWS Config memberikan snapshot konfigurasi dan seberapa sering ia memanggil evaluasi untuk aturan Config periodik.

Jika perintah berhasil, AWS Config tidak mengembalikan output. Untuk memverifikasi pengaturan saluran pengiriman Anda, jalankan describe-delivery-channels perintah.

- Untuk detail API, lihat PutDeliveryChannelDi Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell V4

Contoh 1: Contoh ini mengubah properti DeliveryFrequency dari saluran pengiriman yang ada.

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

- Untuk detail API, lihat PutDeliveryChannelDi Referensi Alat AWS untuk PowerShell Cmdlet (V4).

Alat untuk PowerShell V5

Contoh 1: Contoh ini mengubah properti DeliveryFrequency dari saluran pengiriman yang ada.

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

- Untuk detail API, lihat PutDeliveryChannelDi Referensi Alat AWS untuk PowerShell Cmdlet (V5).

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Config dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Riwayat Dokumen

Tabel berikut menjelaskan perubahan penting pada dokumentasi untuk AWS Config. Untuk notifikasi tentang pembaruan dokumentasi ini, Anda dapat berlangganan ke umpan RSS.

- Versi API: 2014-11-12
- Pembaruan dokumentasi terbaru: 15 Juli 2025

Perubahan	Deskripsi	Tanggal
AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke jenis AWS Backup sumber AWS Manajemen Penagihan dan Biaya daya AWS CloudForm ation Amazon Relationa l Database Service baru CloudFront Resolusi Entitas AWS AWS IoT AWS Private Certificate Authority,,,,,, Amazon S3. Untuk informasi selengkapnya, lihat Jenis sumber daya yang didukung.	Juli 15, 2025
Pembaruan IAM keamanan	`AWS_ConfigRole` Kebijakan dan `AWSConfigServiceRolePolicy` kebijakan sekarang memberikan izin tambahan untuk AWS Backup gateway,, AWS Manajemen Penagihan dan Biaya Amazon Bedrock,, Amazon,,,, CloudFront, Resolusi Entitas AWS, AWS	Juni 18, 2025

	CloudFormation Amazon AWS Private Certificate Authority Redshift AWS IoT Core Device Advisor AWS Lambda AWS Network Manager, Amazon S3 Tables,. Pengaturan Cepat AWS Systems Manager Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	
AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke jenis sumber daya Amazon Bedrock baru. Untuk informasi selengkapnya, lihat Jenis sumber daya yang didukung.	Juni 17, 2025

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • cloudfront-ssl-policy-check • cognito-identity-pool-unauth-akses-cek • ec2- diaktifkan enis-source-destination-check • elbv2- listener-encryption-in-transit • lambda-function-xray-enabled • msk-cluster-public-access-dinonaktifkan • msk-connect-connector-logging-diaktifkan • msk-unrestricted-access-check • aurora-mysql-cluster-audit-logging • redshift-cluster-multi-az-diaktifkan • s3 -aturan-periksa express-dir-bucket-lifecycle • ssm-automation-logging-enabled • ssm-automation-block-public-berbagi	Juni 13, 2025

Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` Kebijakan dan `AWS_ConfigRole` kebijakan sekarang memberikan izin tambahan untuk Amazon Bedrock. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	27 Mei 2025
AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke Integrasi Aplikasi Amazon baru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Inspector, Amazon Macie, Amazon Route 53 Profiles, Amazon Serverless, OpenSearch Amazon Simple Storage Service (Amazon S3),, dan jenis sumber daya Amazon AI. AWS Security Hub SageMaker Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	April 30, 2025
AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: redshift-serverless-default-db-name-check	April 22, 2025
AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: redshift-serverless-default-admin-check	17 April 2025

Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` `AWS_ConfigRole` Kebijakan dan kebijakan sekarang memberikan izin tambahan untuk AWS B2B Pertukaran Data, Amazon Bedrock,, ,, AWS Database Migration Service (AWS DMS) AWS Clean Rooms, Amazon CloudWatch Log AWS CodeConnections AWS Direct Connect, Amazon Macie, Amazon Managed Blockchain, Amazon Q Business, Route 53 Profiles, Amazon Simple Storage Service (Amazon S3), SageMaker Amazon AWS Security Hub AI,, dan, Kontak, dan. Manajer Insiden AWS Systems Manager Manajer Insiden AWS Systems Manager AWS Systems Manager Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	April 8, 2025

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • s3-bucket-tagged • ecr-repository-tagged • sagemaker-feature-group-tagged • sagemaker-domain-tagged • cognito-user-pool-tagged	April 1, 2025

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • nlb-cross-zone-load-menyeimbangkan diaktifkan • redshift-serverless-publish-logske cloudwatch • rds-instance-subnet-igw-periksa • ec2- - spot-fleet-request-ct encryption-at-rest • redshift-serverless-workgroup-encrypted-dalam transit • redshift-serverless-workgroup-no-akses publik • redshift-serverless-namespace-cmk-enkripsi • event-data-store-cmk-enkripsi diaktifkan • ecs-task-definition-network-mode-not-host • rds-proxy-tls-encryption • nlb-logging-enabled • redshift-audit-logging-enabled • s3- lifecycle-policy-check • sagemaker-image-tagged • redshift-cluster-parameter-group-ditandai • ec2- dhcp-options-tagged • sagemaker-app-image-config-ditandai	Maret 22, 2025

- mariadb-publish-logs-to-cloudwatch-log
- docdb-cluster-encrypted-in-transit
- rds-sqlserver-encrypted-in-transit
- ec2- traffic-mirror-session-tagged
- ec2- launch-template-tagged
- ec2- traffic-mirror-target-tagged
- transfer-certificate-tagged
- batch-managed-compute-env-compute-resources-tagged
- lightsail-disk-tagged
- transfer-profile-tagged
- amplify-app-tagged
- ec2- prefix-list-tagged
- amplify-branch-tagged
- transfer-agreement-tagged
- datasync-task-tagged
- transfer-workflow-tagged
- sagemaker_notebook_instance_platform_version
- ec2- traffic-mirror-filter-tagged
- aurora-mysql-cluster-audit-logging
- ssm-document-tagged
- transfer-connector-tagged

- rds-mariadb-instance-encrypted-dalam transit
- iam-saml-provider-tagged
- ec2-fleet-tag
- iam-server-certificate-tagged
- iam-oidc-provider-tagged
- alb-listener-tagged
- glb-listener-tagged
- ec2- -ditandai network-insights-access-scope
- lightsail-certificate-tagged
- ec2- capacity-reservation-tagged
- ec2- -ditandai transit-gateway-multicast-domain
- dms-endpoint-tagged
- ec2- carrier-gateway-tagged
- dms-replication-task-tagged
- ec2- client-vpn-endpoint-tagged
- lightsail-bucket-tagged
- ec2- network-insights-access-scope -analisis ditandai
- nlb-listener-tagged
- ec2- network-insights-path-tagged

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • docdb-cluster-encrypted-in-transit • mariadb-publish-logs-to-cloudwatch-log • aurora-mysql-cluster-audit-logging • rds-mariadb-instance-encrypted-dalam transit • rds-sqlserver-encrypted-in-transit • sagemaker-notebook-instance-platform-versi • appstream-fleet-multi-az • apprunner-vpc-connector-multi-az • mq-broker-general-logging-diaktifkan • mq-active-single-instance-broker-storage-type-efs • mq-active-broker-ldap-otentikasi • iottwinmaker-component-type-tagged	Maret 19, 2025

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • fsx-openzfs-deployment-type-periksa • fsx-ontap-deployment-type-periksa • fsx-windows-deployment-type-periksa • redshift-serverless-workgroup-routes-dalam-vpc	Maret 18, 2025
AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: ec2- -ami instance-launched-with-allowed	Maret 11, 2025

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • connect-instance-logging-enabled • ecr-repository-cmk-encryption-diaktifkan • elbv2- -periksa predefined-security-policy-ssl • glue-spark-job-supported-versi • guardduty-runtime-monitoring-enabled • guardduty-ecs-protection-runtime-diaktifkan • penjaga-ec2- protection-runtime-enabled • netfw-subnet-change-protection-diaktifkan • rds-sql-server-logske cloudwatch • sqs-queue-no-public-akses • transfer-connector-logging-enabled	7 Maret 2025

Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` Kebijakan dan `AWS_ConfigRole` kebijakan sekarang memberikan izin tambahan untuk Amazon Elastic Compute Cloud (Amazon EC2). Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	Maret 4, 2025

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • athena-workgroup-description • amplify-app-tagged • sagemaker-app-image-config-ditandai • elasticbeanstalk-application-version-description • amplify-branch-performance-mode-diaktifkan • athena-workgroup-engine-version-upgrade otomatis • sagemaker-image-description • devicefarm-instance-profile-tagged • transfer-workflow-description • ec2- traffic-mirror-session-tagged • appstream-fleet-in-vpc • transfer-agreement-tagged • ec2- traffic-mirror-target-description • transfer-agreement-description • athena-prepared-statement-description	Februari 8, 2025

- batch-managed-compute-env-compute-resources-tagged
- codedeploy-deployment-group-auto-rollback-diaktifkan
- batch-managed-compute-environment-using-launch-template
- ec2- prefix-list-tagged
- ec2- traffic-mirror-filter-tagged
- athena-workgroup-enforce-workgroup-konfigurasi
- transfer-certificate-tagged
- batch-compute-environment-managed
- lightsail-disk-tagged
- transfer-profile-tagged
- ec2- traffic-mirror-target-tagged
- appintegrations-event-integration-tagged
- datasync-task-tagged
- batch-compute-environment-enabled
- appconfig-configuration-profile-validators-tidak-kosong
- elasticbeanstalk-application-description
- codedeploy-deployment-group-outdated-instances-pembaruan

- ec2- launch-template-tagged
- fis-experiment-template-tagged
- ivs-channel-playback-authorization-diaktifkan
- redshift-cluster-parameter-group-ditandai
- ec2- traffic-mirror-filter-description
- appintegrations-event-integration-description
- athena-data-catalog-description
- fis-experiment-template-log-konfigurasi-ada
- amplify-app-description
- amplify-branch-tagged
- batch-job-queue-enabled
- elasticbeanstalk-environment-description
- amplify-app-branch-auto-penghapusan-diaktifkan
- appconfig-hosted-configuration-version-deskripsi
- appconfig-freeform-profile-config-penyimpanan
- datasync-task-data-verification-diaktifkan
- apprunner-service-observability-enabled
- transfer-certificate-description

	• appconfig-deployment-strategy-replicateuntuk-ssm • transfer-workflow-tagged • transfer-connector-tagged • ec2- traffic-mirror-session-description • customerprofiles-object-type-allow-pembuatan profil • sagemaker-image-tagged	
AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke jenis sumber daya Amazon Simple Storage Service (Amazon S3) yang baru. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	Februari 6, 2025
AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke jenis sumber daya Amazon Simple Storage Service (Amazon S3) yang baru. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	Januari 29, 2025

Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` Kebijakan dan `AWS_ConfigRole` kebijakan sekarang memberikan izin tambahan untuk AWS Clean Rooms, Amazon Comprehend, Amazon Elastic Compute Cloud (Amazon),, EC2 Amazon Simple Storage Service (Amazon S3) AWS HealthOmics, dan Amazon Simple Email Service (Amazon SES). Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	Januari 16, 2025

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • appmesh-mesh-deny-tcp-penerusan • sagemaker-model-isolation-enabled • evidently-project-description • alb-internal-scheme-check • evidently-segment-description • appconfig-environment-description • apprunner-service-in-vpc • sagemaker-domain-in-vpc • nlb-internal-scheme-check • emr-security-configuration-encryption-istirahat • apprunner-service-no-public-akses • sagemaker-model-in-vpc • appconfig-deployment-strategy-description • evidently-launch-description • iot-authorizer-token-signing-diaktifkan	Januari 9, 2025

AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke jenis sumber daya Amazon Elastic Compute Cloud (Amazon EC2) yang baru. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	Januari 9, 2025

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • batch-job-queue-tagged • iottwinmaker-sync-job-tagged • codeguruprofiler-profiling-group-tagged • ivs-recording-configuration-tagged • iottwinmaker-entity-tagged • iottwinmaker-workspace-tagged • iottwinmaker-scene-tagged • acmpca-certificate-authority-tagged • appflow-flow-tagged • iotevents-detector-model-tagged • appmesh-virtual-node-logging-file-path-exists • apprunner-vpc-connector-tagged • apprunner-service-tagged • iotwireless-fuota-task-tagged • appmesh-virtual-node-backend-defaults-tls-on • codegurureviewer-repository-association-tagged • iotevents-input-tagged	Januari 8, 2025

- appmesh-virtual-gateway-logging-file-path-exists
- batch-compute-environment-tagged
- batch-scheduling-policy-tagged
- customerprofiles-object-type-tagged
- emr-security-configuration-encryption-transit
- iotwireless-service-profile-tagged
- ivs-playback-key-pair-ditandai
- cassandra-keyspace-tagged
- iotevents-alarm-model-tagged
- appconfig-application-description
- appmesh-virtual-gateway-backend-default-tls
- ivs-channel-tagged
- iotwireless-multicast-group-tagged

AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke jenis sumber daya Amazon Elastic Compute Cloud (Amazon EC2), Amazon Cognito AWS Elemental MediaConnect, dan OpenSearch Amazon Service yang baru. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	Desember 19, 2024
Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` Kebijakan ini sekarang memberikan izin tambahan untuk. AWS Organizations Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	Desember 18, 2024

AWS Config mendukung perekam konfigurasi terkait layanan	Dengan rilis ini, AWS Config mendukung perekam konfigurasi terkait layanan. Anda mengaktifkan perekam konfigurasi terkait layanan di layanan yang didukung atau menggunakan AWS CLI, dan perekam merekam jenis sumber daya yang diperlukan untuk layanan tertaut atas nama Anda. Anda dapat melihat detail perekam konfigurasi terkait layanan menggunakan AWS Config konsol atau. AWS CLI Untuk informasi selengkapnya, lihat Bekerja dengan perekam konfigurasi.	November 27, 2024

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • appconfig-application-tagged • appconfig-configuration-profile-tagged • appconfig-environment-tagged • appconfig-extension-association-tagged • appmesh-gateway-route-tagged • appmesh-mesh-tagged • appmesh-route-tagged • appmesh-virtual-gateway-tagged • appmesh-virtual-node-tagged • appmesh-virtual-router-tagged • appmesh-virtual-service-tagged • evidently-launch-tagged • evidently-project-tagged • evidently-segment-tagged • frauddetector-entity-type-tagged • frauddetector-label-tagged • frauddetector-outcome-tagged	November 12, 2024

- frauddetector-variable-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged

Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` `AWS_ConfigRole` Kebijakan dan kebijakan sekarang memberikan izin tambahan untuk AWS AppConfig,, Amazon Connect, Amazon AWS CloudTrail, Amazon DevOps Guru,, Identity Store DataZone,,, AWS Glue,, Amazon Interactive Video Service (Amazon IVS) AWS IoT FleetWise AWS IoT Wireless, Amazon CloudWatch Logs, Amazon Observability Access Manager,, Amazon AWS Payment Cryptography Relational Database Service (CloudWatch Amazon RDS), Amazon Rekognition, Amazon Rekognition, Amazon Simple Storage Service (Amazon S3), Amazon Scheduler, dan Amazon VPC Lattice. AWS IoT EventBridge AWS Systems Manager Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	November 8, 2024
AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: cognito-user-pool-advanced-security-enabled	6 November 2024

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • active-mq-supported-version • rabbit-mq-supported-version • ec2- vpn-connection-logging-enabled • appsync-cache-ct-encryption-saat istirahat • appsync-cache-ct-encryption-dalam transit • vpc-endpoint-enabled • efs-filesystem-ct-encrypted • redshift-cluster-subnet-group-multi-az • sns-topic-no-public-akses • rabbit-mq-supported-version • kms-key-policy-no-akses publik • rds-mysql-instance-encrypted-dalam transit • rds-postgres-instance-encrypted-dalam transit • rds-sql-server-logskecloudwatch • ec2- 2-periksa launch-template-imdsv	Oktober 21, 2024

AWS Config mendukung paket kesesuaian baru	Dengan rilis ini, AWS Config mendukung paket kesesuaian berikut: • Praktik Terbaik Operasional untuk PCI DSS 4.0 (Tidak termasuk jenis sumber daya global) • Praktik Terbaik Operasional untuk PCI DSS 4.0 (Termasuk jenis sumber daya global)	September 23, 2024
Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` Kebijakan dan `AWS_ConfigRole` kebijakan sekarang memberikan izin tambahan untuk Amazon OpenSearch Service Severless AppStream, Amazon,,, AWS Backup, EC2 Image Builder AWS CloudTrail AWS Glue AWS IoT, Amazon Interactive Video Service (Amazon IVS),, AWS Elemental MediaConnect,, AWS Elemental MediaTailor, AWS HealthOmics dan Amazon Scheduler. EventBridge Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	September 16, 2024

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • ec2- resources-in-logically-air -gapped-lemari besi • ebs-resources-in-logically-air-gapped-vault • aurora-resources-in-logically-air-gapped-vault • efs-resources-in-logically-air-gapped-vault • s3- resources-in-logically-air -gapped-lemari besi • storagegateway-resources-in-logically-air-gapped-vault • virtualmachine-resources-in-logically-air-gapped-vault	September 3, 2024
AWS Config mendukung paket kesesuaian baru	Dengan rilis ini, AWS Config mendukung paket kesesuaian berikut: • Praktik Terbaik Operasional untuk FedRAMP (Bagian Tinggi 1) • Praktik Terbaik Operasional untuk FedRAMP (Bagian Tinggi 2)	Agustus 27, 2024

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • athena-workgroup-logging-enabled • codebuild-report-group-encrypted-saat istirahat • cognito-user-pool-advanced-keamanan diaktifkan • datasync-task-logging-enabled • efs-automatic-backups-enabled • glue-job-logging-enabled • glue-ml-transform-encrypted-saat istirahat • kinesis-stream-backup-retention-periksa • rds-aurora-postgresql-logske cloudwatch • rds-postgresql-logs-to-jamtangan awan • workspaces-root-volume-encryption-diaktifkan • workspaces-user-volume-encryption-diaktifkan	Juli 22, 2024

Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` Kebijakan dan `AWS_ConfigRole` kebijakan tersebut sekarang memberikan izin tambahan untuk Amazon Elastic File System (Amazon EFS), Amazon Manajer Sistem AWS untuk SAP Redshift, dan. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	Juni 17, 2024
AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • cloudtrail-s3- bucket-public-access-prohibited • cloudtrail-s3- bucket-access-logging	8 Mei 2024
AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: iam-external-access-analyzer-enabled	2 Mei 2024

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • guardduty-malware-protection-enabled • guardduty-rds-protection-enabled • guardduty-s3-protection-enabled • inspector-lambda-standard-scan-diaktifkan	April 26, 2024
AWS Config menyederhanakan analisis penggunaan dengan Amazon CloudWatch	Dengan rilis ini, CloudWatch metrik Amazon untuk memantau penggunaan AWS Config data hanya akan menampilkan penggunaan yang dapat ditagih. Ini berarti, penggunaan yang tidak dapat ditagih tidak akan lagi ditampilkan di CloudWatch metrik Amazon yang dipancarkan ke dan konsol. AWS Config AWS Config Ini memungkinkan Anda memvalidasi AWS Config penyiapan dan penggunaan menggunakan CloudWatch metrik Amazon dan menghubungkan penggunaan yang dapat ditagih dengan biaya terkait. Untuk informasi selengkapnya, lihat Metrik AWS Config Penggunaan dan Sukses.	April 26, 2024

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: iam-server-certificate-expiration-check	April 23, 2024
AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • vpc-sg-port-restriction-periksa • cloudtrail-all-write-s3- data-event-check • cloudtrail-all-read-s3- data-event-check	April 17, 2024
AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • guardduty-eks-protection-audit-diaktifkan • guardduty-eks-protection-runtime-diaktifkan • guardduty-lambda-protection-enabled • inspector-ec2-scan-enabled • inspector-ecr-scan-enabled • inspector-lambda-code-scan-diaktifkan • redshift-unrestricted-port-access	16 April 2024

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: efs-mount-target-public-accessible	Maret 20, 2024
AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • dms-neptune-iam-authorization-diaktifkan • dms-mongo-db-authentication-diaktifkan • dms-redis-tls-enabled • dax-tls-endpoint-encryption • eks-cluster-secrets-encrypted • kinesis-firehose-delivery-stream-dienkripsi • mq-cloudwatch-audit-log-diaktifkan • mq-cloudwatch-audit-log-diaktifkan • opensearch-primary-node-fault-toleransi • sagemaker-endpoint-config-prod-hitungan contoh • service-catalog-shared-within-organisasi • transfer-family-server-no-ftp	Februari 26, 2024

Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` Kebijakan dan `AWS_ConfigRole` kebijakan sekarang memberikan izin tambahan untuk Amazon Managed Service untuk Prometheus, Amazon, Amazon CloudWatch Cognito, Amazon, Amazon,, (AWS Identity and Access Management IAM),, ElastiCache, FSx Amazon AWS RAM Redshift Serverless AWS Glue, Amazon AI, dan AWS Lambda Amazon Simple Notification Service (Amazon SNS). SageMaker Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	Februari 22, 2024
AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: s3- -enabled bucket-cross-region-replication	Februari 12, 2024

AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke yang baru AWS AppConfig, Amazon CloudWatch Terbukti, AWS Identity and Access Management (IAM), Amazon MemoryDB (MemoryDB), Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Redshift, dan jenis sumber daya. AWS Transfer Family Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	Februari 6, 2024
AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: macie-auto-sensitive-data-discovery-check	Januari 29, 2024

AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke Amazon baru AppStream, AWS Key Management Service (AWS KMS), Amazon Relational Database Service (Amazon RDS), Amazon Cognito, Amazon Elastic Compute Cloud (Amazon), Image EC2 Builder EC2,,, Amazon, AWS Ground Station AWS Mainframe Modernization QuickSight Amazon Redshift, dan jenis sumber daya. AWS Systems Manager Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	Januari 3, 2024

Batas layanan meningkat untuk jumlah maksimum AWS Config Aturan per Wilayah per akun	Dengan rilis ini, AWS Config mendukung 1000 AWS Config aturan per AWS Wilayah per akun. Peningkatan ini berlaku untuk total semua aturan yang diterapkan termasuk aturan AWS Config terkelola, aturan AWS Config khusus, paket AWS Config kesesuaian, AWS Security Hub kontrol, AWS Firewall Manager k ebijakan, dan rencana AWS Backup cadangan per Wilayah per akun. Untuk informasi selengkapnya, lihat Batas Layanan.	Desember 19, 2023

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • s3- meets-restore-time-target • ebs-meets-restore-time-target • ec2- meets-restore-time-target • rds-meets-restore-time-target • efs-meets-restore-time-target • fsx-meets-restore-time-target • aurora-meets-restore-time-target • dynamodb-meets-restore-time-target	Desember 19, 2023

Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` Kebijakan dan `AWS_ConfigRole` kebijakan sekarang memberikan izin tambahan untuk AWS AppConfig, Amazon Managed Service for Prometheus, () AWS Database Migration Service ,AWS DMS(AWS Identity and Access Management) IAM, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Logs, dan Amazon Simple Storage Service (CloudWatch Amazon S3). AWS Organizations Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	5 Desember 2023

Rilis pratinjau: Prosesor kueri bahasa alami untuk kueri lanjutan	Dengan rilis ini, Anda dapat menggunakan prosesor kueri bahasa alami untuk kueri lanjutan, yang menggunakan kemampuan kecerdasan buatan generatif (AI generatif) yang memungkinkan Anda mengajukan pertanyaan dalam bahasa Inggris biasa dan mengubahnya menjadi ready-to-use format kueri. Dengan prosesor kueri bahasa alami, Anda dapat melakukan kueri Akun AWS atau di seluruh AWS organisasi. Untuk informasi selengkapnya, lihat Pemroses kueri bahasa alami untuk kueri lanjutan.	26 November 2023

Rekaman berkala	Dengan rilis ini, AWS Config mendukung perekaman berkala. Perekaman berkala memberi Anda kemampuan untuk menangkap perubahan konfigurasi terbaru untuk sumber daya Anda selama periode waktu tertentu. Anda sekarang dapat mengatur frekuensi default untuk perekam konfigurasi ke Harian, memungkinkan Anda menerima item konfigurasi (CI) yang mewakili status terbaru sumber daya Anda selama periode 24 jam terakhir, hanya jika berbeda dari CI sebelumnya yang direkam. AWS Config Konsol juga memperkenalkan pengalaman strategi perekaman baru, di mana Anda juga dapat mengganti frekuensi perekaman untuk jenis sumber daya tertentu atau mengecualikan jenis sumber daya tertentu dari perekaman. Ini dapat membantu membuat pengaturan Anda sesuai dengan kebutuhan granular Anda. Tipe data berikut ditambahkan: • RecordingMode • RecordingModeOverride	26 November 2023

Tipe data berikut diperbarui:

- PutConfigurationRecorder
- ConfigurationRecorder
- BaseConfigurationItem
- ConfigurationItem

Halaman-halaman berikut dalam panduan pengembang diperbarui:

- Sumber Daya Pengodean Ulang AWS
- Menyiapkan AWS Config dengan AWS Config Konsol | Pengaturan 1-klik
- Menyiapkan AWS Config dengan AWS Config Konsol | Pengaturan manual
- Menyiapkan AWS Config dengan AWS CLI

Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` Kebijakan dan `AWS_ConfigRole` kebijakan sekarang memberikan izin tambahan untuk Amazon Cognito, Amazon Connect, Amazon EMR,, Amazon MemoryDB, AWS Ground Station, Amazon AWS Mainframe Modernization, Amazon, Amazon Relational Database QuickSight Service (Amazon RDS) AWS Organizations, Amazon Redshift, Amazon Route 53, dan. AWS Service Catalog AWS Transfer Family `AWSConfigServiceRolePolicy` Kebijakan dan `AWS_ConfigRole` kebijakan juga sekarang menambahkan pengidentifikasi keamanan (SID) untuk`AWSConfigServiceRolePolicyStatementID` ,,`AWSConfigSLRLogStatementID` , `AWSConfigSLRLogEventStatementID` `AWSConfigSLRApiGatewayStatementID` , dan `AWSConfigServiceRolePolicy` kebijakan.	17 November 2023

Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • acm-pca-root-ca-dinonaktifkan • dynamodb-table-deletion-protection-diaktifkan • ec2- diaktifkan client-vpn-connection-log • eks-cluster-log-enabled • emr-block-public-access • fsx-windows-audit-log-dikonfigurasi • fsx-openzfs-copy-tags-diaktifkan • fsx-lustre-copy-tagsuntuk-backup • msk-enhanced-monitoring-enabled • mq-auto-minor-version-upgrade diaktifkan • neptune-cluster-multi-az-diaktifkan • opensearch-update-check • s3- -hanya access-point-in-vpc • s3- -blok access-point-public-access • s3- bucket-mfa-delete-enabled	9 November 2023

AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke new AWS Identity and Access Management (IAM),, (),, Amazon Connect AWS Network Manager AWS App Mesh, Amazon Elastic Compute Cloud AWS Private Certificate Authority (AWS Private CA Amazon EC2), Amazon Elastic Container Service (Amazon ECS) AWS IoT,, AWS IoT TwinMaker, Amazon Managed Streaming untuk Apache Kafka Connect (Amazon MSK Connect),, dan jenis sumber daya. AWS Lambda Penjelajah Sumber Daya AWS Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	3 November 2023
AWS Config mendukung paket kesesuaian baru	Dengan rilis ini, AWS Config update paket kesesuaia n berikut: Praktik Terbaik Operasional untuk BNM T RMi	26 Oktober 2023

Dasbor Kepatuhan dan Inventaris untuk Agregator	Dengan rilis ini, AWS Config tambahkan halaman dasbor kepatuhan dan halaman dasbor inventaris ke tampilan agregat di AWS Config konsol. Untuk halaman dasbor kepatuhan, Anda dapat melihat dasbor otomatis dengan widget yang merangkum wawasan tentang kepatuhan sumber daya dalam agregator Anda, seperti 10 jenis sumber daya teratas berdasarkan sumber daya yang tidak sesuai, 10 paket kesesuaian tingkat akun teratas menurut aturan yang tidak sesuai, dan banyak lagi. Untuk halaman dasbor inventaris, Anda dapat melihat dasbor otomatis dengan widget yang merangkum wawasan tentang data konfigurasi sumber daya dalam agregator Anda, seperti 10 jenis sumber daya teratas berdasarkan jumlah sumber daya, 10 akun teratas berdasarkan jumlah sumber daya, dan banyak lagi. Untuk informasi tentang grafik dan bagan, lihat Dasbor kepatuhan dan dasbor Inventaris.	23 Oktober 2023

Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` `AWS_ConfigRole` Kebijakan dan kebijakan sekarang memberikan izin tambahan untuk AWS Private CA,, Amazon Connect AWS App Mesh, Amazon Elastic Container Service (Amazon ECS), Amazon CloudWatch Jelas, Amazon Managed Grafana, Amazon, Amazon Inspector,, GuardDuty, Amazon AWS IoT Managed AWS IoT TwinMaker Streaming untuk Apache Kafka (Amazon MSK),,,, dan Amazon AI. AWS Lambda AWS Network Manager AWS Organizations SageMaker Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	4 Oktober 2023

AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke jenis sumber daya baru AWS IoT,, AWS IoT TwinMaker AWS IoT Wireless, Amazon Personali sasi Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon AWS CodeBuild AI,, SageMaker Amazon, dan AppStream Amazon Inspector. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	4 Oktober 2023

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • docdb-cluster-deletion-protection-diaktifkan • docdb-cluster-audit-logging-diaktifkan • docdb-cluster-snapshot-public-dilarang • mq-active-deployment-mode • mq-rabbit-deployment-mode • dms-auto-minor-version-tingkatkan periksa • dms-replication-task-target db-logging • dms-replication-task-source db-logging • dms-endpoint-ssl-configured • custom-eventbus-policy-attached • global-endpoint-event-replication-diaktifkan • rute53- query-logging-enabled • rds-aurora-mysql-audit-logging-diaktifkan • rds-cluster-auto-minor-version-upgrade-enable • appsync-authorization-check • netfw-deletion-protection-enabled	21 September 2023

	• wafv2- rulegroup-logging-enabled • msk-in-cluster-node-membutuhkan-tls	
AWS Config mendukung paket kesesuaian baru	Dengan rilis ini, AWS Config update paket kesesuaian berikut: • Praktik Terbaik Operasional untuk Amazon S3 • Praktik Terbaik Operasional untuk EC2	September 8, 2023
Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` Kebijakan ini sekarang menghapus izin untuk AWS Systems Manager (Systems Manager). Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	September 6, 2023
AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke Amazon CodeGuru Profiler,, AWS Elemental MediaConnect AWS Transfer Family, Amazon Managed Service baru untuk Prometheus AWS Batch,,, dan jenis sumber daya. AWS Cloud Map Amazon Route 53 Resolver Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	September 6, 2023

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • athena-workgroup-encrypted-at-istirahat • neptune-cluster-iam-database-otentikasi • neptune-cluster-copy-tags-to-snapshot-enabled • neptune-cluster-cloudwatch-log-ekspor diaktifkan • neptune-cluster-deletion-protection-diaktifkan • neptune-cluster-snapshot-encrypted • neptune-cluster-backup-retention-periksa • neptune-cluster-encrypted • neptune-cluster-snapshot-public-dilarang • docdb-cluster-backup-retention-periksa • docdb-cluster-encrypted • rds-cluster-encrypted-at-istirahat	10 Agustus 2023

AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke baru AWS Amplify, Amazon,, Amazon Athena AppIntegrations AWS App Mesh, Amazon Elastic Compute Cloud (Amazon), Amazon CloudWatch Terbukti EC2, Amazon Forecast,,,,, Amazon Managed Streaming untuk Apache Kafka Kafka (AWS Elemental MediaTailor Amazon MSK) AWS Elemental MediaConvert, Amazon Personalisasi, Amazon Pinpoint, dan jenis sumber daya. AWS IoT Greengras s Version 2 AWS Ground Station AWS Resilience Hub Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	3 Agustus 2023

Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` `AWS_ConfigRole` Kebijakan dan kebijakan sekarang memberikan izin tambahan untuk Alur Kerja Terkelola Amazon untuk, Amazon AppStream 2.0,, AWS App Mesh Amazon,, AWS CloudFormation Amazon Connect CloudFront AWS CodeArtifact,, Amazon AWS CodeBuild, AWS Identity and Access Management (IAM), AWS Glue Amazon Inspector GuardDuty,,,, Amazon Managed Streaming untuk Apache Kafka AWS IoT AWS IoT TwinMaker, AWS IoT Wireless Amazon AWS Elemental MediaConnect Macie,,,, Amazon Route 53, Amazon Simple Storage Service (Amazon S3) Storage Service S3) AWS Network Manager AWS Organizations Penjelajah Sumber Daya AWS, Amazon Simple Notification Service (Amazon SNS), dan Amazon EC2 Systems Manager (SSM). Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	28 Juli 2023

AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke Amazon Kinesis baru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Pinpoint, Amazon Simple Storage Service (Amazon S3) Simple Storage S3), Amazon Virtual Private Cloud (Amazon VPC), Amazon Kendra, Amazon AWS CloudFormation Connect AWS AppConfig,,,,,, dan () sumber daya jenis. AWS App Mesh AWS App Runner AWS Database Migration Service AWS DMS Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	Juli 10, 2023
Batas layanan meningkat untuk paket kesesuaian organisasi	Dengan rilis ini, AWS Config mendukung 350 AWS Config aturan per wilayah per akun di semua paket kesesuaian dan 350 AWS Config aturan organisasi per organisasi. Untuk informasi selengkapnya, lihat Batas Layanan.	13 Juni 2023

Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` `AWS_ConfigRole` Kebijakan dan kebijakan sekarang memberikan izin tambahan untuk Alur Kerja Terkelola Amazon untuk, Amazon Connect AWS Amplify,, Layanan Terkelola AWS App Mesh Amazon untuk Prometheus, Amazon Athena,,,,, Amazon,, Amazon AWS Directory Service DynamoDB AWS Batch AWS CloudFormation AWS CodeArtifact, AWS CloudTrail Amazon Elastic Compute Cloud (CodeGuruAmazon), Amazon Terbukti, Amazon AWS Organizations Forecast,,,,, (AWS Identity and Access Management IAM), CloudWatch Amazon Managed Streaming untuk Apache Kafka AWS Ground Station(AWS IoT Greengrass Amazon MSK), Amazon Lightsail, Amazon Log,, EC2 CloudWatch AWS Elemental MediaConnect AWS Elemental MediaTailor, Amazon Pinpoint, Amazon Virtual Private Cloud (Amazon VPC), Amazon Personalize, Amazon, QuickSight, Amazon Simple Storage	13 Juni 2023

Service (AWS Migration Hub Refactor Spaces Amazon S3), Amazon AI, dan. SageMaker AWS Transfer Family Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.

AWS Config Merekam Pengecualian berdasarkan Jenis Sumber Daya	Dengan rilis ini, AWS Config Anda dapat mengecualikan jenis AWS sumber daya tertentu dari pelacakan inventaris dan pemantaua n kepatuhan sambil tetap melacak semua jenis sumber daya lain yang didukung saat ini tersedia AWS Config, termasuk yang akan ditambahkan di masa mendatang. Anda dapat menggunakan fitur ini untuk berkonsentrasi pada sumber daya penting yang tunduk pada standar kepatuhan dan tata kelola Anda. Pembaruan API untuk perekam konfigurasi dan grup perekaman kompatibe l ke belakang, artinya mereka bekerja dengan versi PutConfigurationRecorderAPI sebelumnya. Anda dapat terus mengelola jenis sumber daya mana yang direkam dengan cara yang sama persis seperti sebelumnya tanpa menggunak an yang diperbarui atau yang baru APIs. Tipe data berikut ditambahkan: • RecordingStrategy • ExclusionByResourceTypes	9 Juni 2023

Tipe data berikut diperbarui:

- PutConfigurationRecorder
- ConfigurationRecorder
- RecordingGroup

Halaman berikut dalam panduan pengembang diperbarui:

- Memilih Sumber Daya Yang Tercatat

AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke Amazon Elastic Container Service (Amazon ECS) baru, Amazon Keyspaces (untuk Apache Cassandra) (Amazon Keyspaces),,,,,, Amazon 2.0 AWS Amplify,, AWS App Mesh Amazon Elastic Compute Cloud (AppStream Amazon AWS Signer) AWS CodeArtif act, Amazon Terbukti, Amazon Forecast, AWS Identity and Access Management (IAM EC2), CloudWatch Amazon Pinpoint Jenis sumber daya Pinpoint, Amazon AI,, Amazon Data Firehose. AWS App Runner SageMaker AWS Transfer Family Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	Juni 5, 2023

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • cloudfront-s3- origin-access-control-enabled • custom-schema-registry-policy-Terlampir • ec2- -semua client-vpn-not-authorize • elasticache-supported-engine-version • macie-status-check • mq-automatic-minor-version-upgrade diaktifkan • mq-cloudwatch-audit-logging-diaktifkan • netfw-logging-enabled • opensearch-encrypted-at-res • step-functions-state-machine-logging-diaktifkan	10 Mei 2023

AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke baru Amazon Route 53 Resolver, Amazon Elastic Compute Cloud (Amazon EC2), AWS IoT Nirkabel,,, AWS Network Manager, AWS Device Farm, Amazon AWS Ground Station, Amazon Redshift AppFlow, Amazon Pinpoint, AWS IoT,, AWS AppConfig EC2 Image Builder, Amazon,, Amazon SageMaker Runtime CloudWatch AWS Panorama, Amazon ECR, dan jenis sumber daya. AWS Audit Manager Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	5 Mei 2023
AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke`AWS::NetworkFirewall::TLSInspectionConfiguration` . Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	1 Mei 2023

Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` `AWS_ConfigRole` Kebijakan dan kebijakan sekarang memberikan izin tambahan untuk Alur Kerja Terkelola Amazon untuk AWS Amplify,, , AWS App Runner Amazon AWS App Mesh CloudFront, AWS CodeArtifact Amazon Elastic Compute Cloud, Amazon Kendra, Amazon Macie, Amazon Route 53, Amazon SageMaker AI, Amazon Pinpoint, AWS Transfer Family, AWS Resilience Hub, Amazon AWS Migration Hub, Directory Service, dan. CloudWatch AWS AWS WAF Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	13 April 2023

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • elasticache-auto-minor-version-tingkatkan periksa • elasticache-repl-grp-auto-failover-diaktifkan • elasticache-repl-grp-encrypted-saat istirahat • elasticache-repl-grp-encrypted-dalam transit • elasticache-repl-grp-redis-auth-diaktifkan • elasticache-subnet-group-check • cloudfront-s3- origin-non-existent-bucket	10 April 2023
Batas layanan meningkat untuk paket kesesuaian organisasi	Dengan rilis ini, AWS Config mendukung 350 AWS Config aturan per akun di semua paket kesesuaian organisasi. Untuk informasi selengkapnya, lihat Batas Layanan.	3 April 2023

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • acm-certificate-rsa-check • appsync-associated-with-waf • appsync-logging-enabled • elasticache-rbac-auth-enabled • mq-no-public-access • netfw-multi-az-enabled • ses-malware-scanning-enabled • eks-cluster-logging-enabled • appsync-cache-encryption-at-istirahat	3 April 2023

AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke Amazon AppStream 2.0 baru, AWS Auto Scaling, Amazon Connect Amazon Elastic Compute Cloud, Amazon,, HealthLake Kinesis video stream EventBridge, Lookout AWS IoT TwinMaker for Vision, Network Manager, Amazon Pinpoint, Amazon Application Recovery Controller (ARC), dan jenis sumber daya. AWS RoboMaker Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	3 April 2023

Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` `AWS_ConfigRole` Kebijakan dan kebijakan sekarang memberikan izin tambahan untuk Alur Kerja Terkelola Amazon untuk Amazon AppFlow,, Amazon AppStream 2.0,, AWS App Runner Amazon,,,, CloudWatch AWS CodeArtifact, AWS CloudFormation CloudFront Amazon Elastic Compute Cloud (AWS Device Farm Amazon) AWS CodeCommit, Amazon CloudWatch Terbukti EC2, Amazon Forecast,, AWS Identity and Access Management (IAM), AWS Ground Station, Amazon MemoryDB, AWS IoT Amazon Pinpoint,,, Amazon AWS Panorama Relational Database Service (AWS Network Manager Amazon RDS), Amazon Redshift, dan Amazon AI. SageMaker Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	30 Maret 2023

Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` Kebijakan dan `AWS_ConfigRole` kebijakan sekarang memberikan izin tambahan untuk AWS Audit Manager. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	3 Maret 2023
AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke baru AWS Elemental MediaPackage, Amazon,, (Amazon EventBridge Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud EC2 (Amazon), Amazon Lookout for Metrics, Amazon AWS Device Farm Lex,,, AWS Budgets Amazon Reviewer,, dan jenis sumber CodeGuru daya. AWS IoT Amazon Route 53 Resolver AWS RoboMaker Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	2 Maret 2023

Pembaruan IAM keamanan	AWS Config sekarang melacak perubahan `AWSConfigMultiAccountSetupPolicy` kebijakan. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	27 Februari 2023
AWS Config Cakupan Sumber Daya berdasarkan Ketersediaan Wilayah	Dengan rilis ini, AWS Config berikan informasi Wilayah untuk setiap jenis sumber daya yang didukung. Untuk informasi tentang jenis sumber daya yang didukung di Wilayah mana, lihat Cakupan Sumber Daya menurut Ketersediaan Wilayah.	Februari 20, 2023

AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke Amazon Interactive Video Service (Amazon IVS) baru, Amazon Simple Storage Service (Amazon S3), Amazon Elastic Kubernetes Service AWS Glue(Amazon EKS), Amazon Relational Database Service (Amazon EKS),, Amazon Relational Database Service (Amazon AWS IoT RDS), dan Managed Service for Jenis sumber daya Apache Flink. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	7 Februari 2023

Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` `AWS_ConfigRole` Kebijakan dan kebijakan sekarang memberikan izin tambahan untuk Alur Kerja Terkelola Amazon untuk Apache Airflow, AWS IoT Amazon 2.0, Amazon CodeGuru Reviewer, AppStream , Amazon Kinesis AWS HealthLake Video Streams, Amazon Application Recovery Controller (ARC), Amazon Elastic Compute Cloud (AWS Device Farm Amazon), Amazon Pinpoint, (IAM EC2), Amazon AWS Identity and Access Management , dan Log Amazon. GuardDuty CloudWatch Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	1 Februari 2023
Pembaruan IAM keamanan	Sebagai praktik terbaik keamanan, `ConfigConformsServiceRolePolicy` kebijakan ini sekarang menghapus izin tingkat sumber daya yang luas untuk. `config:DescribeConfigRules` Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	Januari 12, 2023

Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` `AWS_ConfigRole` Kebijakan dan kebijakan sekarang memberikan izin tambahan untuk Amazon Managed Service untuk Prometheus AWS Audit Manager,,, AWS Device Farm(),, Amazon Elastic Compute Cloud AWS Database Migration Service (Amazon AWS DMS), AWS Directory Service,, Amazon AWS IoT Lightsail,, Amazon EC2, AWS Glue, Amazon Application Recovery Controller (ARC) AWS Elemental MediaPackage QuickSight, AWS Network Manager Amazon Simple Storage Service (AWS Resource Access Manager Amazon S3), dan Amazon Timestream. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	10 Januari 2023

AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke Amazon MQ baru,,, Amazon Fraud Detector AWS AppConfig, EventBridge , AWS Cloud9 Amazon AWS IoT Analytics Lightsail, () AWS IoT, Amazon Application Recovery Controller AWS Elemental MediaPackage (ARCMediaPackage), dan jenis sumber daya. AWS Resilience Hub AWS Transfer Family Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	5 Januari 2023
AWS Config cakupan sumber daya aturan	Dengan rilis ini, AWS Config menampilkan cakupan jenis sumber daya untuk peningkatan jumlah aturan AWS Config terkelola.	21 Desember 2022
AWS Config aturan dapat ditemukan	Dengan rilis ini, AWS Config mendukung halaman untuk Daftar Aturan AWS Config Terkelola menurut Mode Evaluasi, Daftar Aturan AWS Config Terkelola berdasarkan Jenis Pemicu, dan Daftar Aturan AWS Config Terkelola menurut Ketersediaan Wilayah.	21 Desember 2022

AWS Config mendukung paket kesesuaian baru	Dengan rilis ini, AWS Config update paket kesesuaian berikut: • Praktik Terbaik Operasional untuk K-ISMS • Praktik Terbaik Operasional untuk NIST 800 171 • Praktik Terbaik Operasional untuk PCI DSS 3.2.1 • Praktik Terbaik Operasional untuk Esquema Nacional de Seguridad (ENS) High • Praktik Terbaik Operasional untuk Medium Esquema Nacional de Seguridad (ENS) • Praktik Terbaik Operasional untuk Esquema Nacional de Seguridad (ENS) Rendah • Praktik Terbaik Operasional untuk NZISM • Praktik Terbaik Operasional untuk NIST 800-53 rev 5	19 Desember 2022

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • api-gwv2- access-logs-enabled • api-gwv2- authorization-type-configured • cloudfront-security-policy-check • ec2- launch-template-public-ip -dinonaktifkan • elastic-beanstalk-logs-to-jam tangan awan • sagemaker-notebook-instance-inside-vpc • sagemaker-notebook-instance-root-akses-cek • security-account-informatio n-provided • storagegateway-resources-protected-by-rencana cadangan • wafv2- rulegroup-not-empty • wafv2- webacl-not-empty	Desember 9, 2022

AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke Amazon CloudWatch RUM, Amazon, Amazon EventBridge GuardDuty, Amazon Simple Email Service (Amazon SES) AWS Backup,, AWS DataSync, AWS Fault Injection Service dan AWS FIS() jenis sumber daya baru. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	Desember 9, 2022

AWS Config Kepatuhan Proaktif	Dengan rilis ini, AWS Config mendukung kemampuan untuk secara proaktif memeriksa kepatuhan terhadap AWS Config aturan sebelum penyediaan sumber daya. Ini memungkinkan Anda untuk mengevaluasi pengaturan konfigurasi sumber daya Anda sebelum dibuat atau diperbaru i. Gunakan AWS Config untuk melacak perubahan konfigurasi yang dibuat pada sumber daya Anda, baik pra-penyediaan atau pasca-pen yediaan, dan periksa apakah sumber daya Anda cocok dengan konfigurasi yang Anda inginkan. Tipe data berikut ditambahkan: • GetResourceEvaluat ionSummary • StartResourceEvaluation • ListResourceEvaluations Tipe data berikut diperbarui: • DescribeConfigRulesFilters • GetComplianceDetai lsByResource • EvaluationResultQualifier • EvaluationModeConf iguration	28 November 2022

Halaman-halaman berikut dalam panduan pengembang diperbarui:

- Komponen AWS Config Aturan
- Mode Evaluasi dan Jenis Pemicu untuk AWS Config Aturan
- AWS Config Aturan Terkelola
- AWS Config Aturan Kustom
- Mengelola AWS Config Aturan Anda

Deteksi Drift sebagai Item Konfigurasi (CI) untuk Perekam AWS Config Konfigurasi	Dengan rilis ini, AWS Config lacak semua perubahan pada perekam konfigurasi untuk menunjukkan apakah status perekam konfigurasi berbeda, atau telah melayang, dari keadaan sebelumnya; misalnya, jika ada pembaruan ke jenis sumber daya yang telah Anda aktifkan AWS Config untuk dilacak, jika Anda telah menghentikan atau memulai perekam konfigura si, atau jika Anda telah menghapus atau menghapus perekam konfigurasi. Jenis `AWS::Config::Confi gurationRecorder` sumber daya adalah jenis sumber daya sistem AWS Config dan perekaman jenis sumber daya ini diaktifka n secara default di semua Wilayah yang didukung. Perekaman untuk jenis `AWS::Config::Confi gurationRecorder` sumber daya dilengkapi tanpa biaya tambahan. Untuk informasi selengkapnya, lihat Deteksi Drift untuk Perekam Konfigurasi.	18 November 2022

AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke jenis sumber daya baru AWS IoT Events, EC2 Image Builder AWS Cloud Map,, AWS DataSync AWS Glue, Amazon Applicati on Recovery Controller (ARC), dan Amazon Elastic Container Registry (Amazon ECR). Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	8 November 2022
Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` Kebijakan dan `AWS_ConfigRole` kebijakan sekarang memberikan izin tambahan untuk AWS CloudFormation. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	7 November 2022

AWS Config mendukung paket kesesuaian baru	Dengan rilis ini, AWS Config mendukung paket kesesuaian berikut: • Praktik Terbaik Operasional untuk Layanan Informasi Peradilan Pidana (CJIS) • Praktik Terbaik Keamanan untuk Amazon SageMaker AI • Praktik Terbaik Keamanan untuk Amazon Elastic Container Registry Paket kesesuaian berikut diperbarui: • Praktik Terbaik Operasional untuk MAS TRMG • Praktik Terbaik Operasional untuk Kerangka Penilaian Cyber NCSC • Praktik Terbaik Operasional untuk Prinsip Keamanan Cloud NCSC	27 Oktober 2022

Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` `AWS_ConfigRole` Kebijakan dan kebijakan sekarang memberikan izin tambahan untuk AWS Certificate Manager, Alur Kerja Terkelola Amazon untuk Apache Airflow,,, AWS Amplify Amazon Keyspaces, AWS AppConfig Amazon, Amazon Connect,, CloudWatch Amazon Elastic Compute Cloud (Amazon) AWS Glue DataBrew, Amazon EC2 Elastic Kubernetes Service (Amazon EKS), Amazon,, Amazon Fraud AWS Fault Injection Service Detector, Amazon, Server Amazon, Layanan Lokasi EventBridge Amazon Service,, Amazon Lex FSx, GameLift Amazon Lightsail, Amazon AWS IoT Pinpoint,,,, Amazon OpsWorks AWS Panorama AWS Resource Access Manager QuickSight, Amazon Relational Database Service (Amazon RDS), Amazon Rekognition,,, Amazon Route 53 AWS RoboMaker AWS Resource Groups, Amazon Simple Storage Service (Amazon S3),, dan. AWS Cloud Map AWS Security Token Service	Oktober 19, 2022

	Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	
AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke Amazon Elastic Compute Cloud (Amazon EC2) baru, Amazon Simple Email Service (Amazon SES) AWS AppConfig,, AWS Cloud Map, AWS DataSync dan jenis sumber daya. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	6 Oktober 2022
AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke Amazon GuardDuty, Amazon SageMaker AI,,, AWS AppSync AWS Cloud Map, dan jenis AWS DataSync sumber daya baru. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	4 Oktober 2022
AWS Config mendukung paket kesesuaian baru	Dengan rilis ini, AWS Config update paket kesesuaian Praktik Terbaik Operasional untuk SWIFT CSP.	4 Oktober 2022

AWS Config mendukung paket kesesuaian baru	Dengan rilis ini, AWS Config mendukung paket kesesuaian berikut: • Praktik Terbaik Operasional untuk CMMC 2.0 Level 1 • Praktik Terbaik Operasional untuk CMMC 2.0 Level 2 Paket kesesuaian berikut diperbarui: • Praktik Terbaik Operasional untuk Amazon API Gateway • Praktik Terbaik Operasional untuk Pilar Keandalan AWS Kerangka Kerja yang Dirancang dengan Baik • Praktik Terbaik Operasional untuk Pilar Keamanan AWS Kerangka Well-Architected • Praktik Terbaik Operasional untuk CMMC Level 1 • Praktik Terbaik Operasional untuk CMMC Level 2 • Praktik Terbaik Operasional untuk CMMC Level 3 • Praktik Terbaik Operasional untuk CMMC Level 4 • Praktik Terbaik Operasional untuk CMMC Level 5 • Praktik Terbaik Operasional untuk FFIEC	30 September 2022

	• Praktik Terbaik Operasional untuk FedRAMP (Rendah) • Praktik Terbaik Operasional untuk Pemberitahuan MAS 655 • Praktik Terbaik Operasional untuk NBC TRMG • Praktik Terbaik Operasional untuk NIST 800 172	
Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` Kebijakan dan `AWS_ConfigRole` kebijakan sekarang memberikan izin tambahan untuk AWS Glue. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	14 September 2022
AWS Config mendukung paket kesesuaian baru	Dengan rilis ini, AWS Config mendukung paket kesesuaian Praktik Terbaik Operasional untuk SWIFT CSP.	9 September 2022

Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` `AWS_ConfigRole` Kebijakan dan kebijakan tersebut sekarang memberikan izin tambahan untuk Amazon AppFlow, Amazon, Amazon CloudWatch RUM CloudWatch, Amazon CloudWatch Synthetics, Profil Pelanggan Amazon Connect, ID Suara Amazon Connect, Amazon Guru, Amazon DevOps Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon, EventBridge Skema Amazon,, Detektor Fraud Detector Amazon EventBridge, Server Amazon FinSpace Amazon, Amazon Interactive Layanan Video (Amazon IVS) GameLift , Layanan Terkelola Amazon untuk Apache Flink, Image Builder EC2 , Amazon Lex, Amazon Lightsail, Layanan Lokasi Amazon, Amazon Lookout for Equipment, Amazon Lookout untuk Metrik, Amazon Lookout for Vision, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon QuickSight Nimble Pinpoint, Amazon, Amazon StudioAmazon , Pemulihan Aplikasi	7 September 2022

Amazon Pengontrol (ARC),, Layanan Penyimpanan Sederhana Amazon (Amazon S3) Simple Storage S3), Amazon Route 53 Resolver Amazon SimpleDB, Layanan Email Sederhana Amazon (Amazon SES), Amazon Timestream,,,,,,,,, AWS AppConfig AWS AppSync AWS Auto Scaling AWS Backup AWS Budgets AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT, AWS IoT Analytics , AWS IoT Events, AWS IoT SiteWise, AWS IoT TwinMaker , AWS Lake Formation, AWS License Manager, AWS Resilience Hub, AWS Signer, dan AWS Transfer Family. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.

AWS Config mendukung paket kesesuaian baru	Dengan rilis ini, AWS Config mendukung paket kesesuaian berikut: • Praktik Terbaik Operasional untuk Amazon CloudWatch • Praktik Terbaik Operasional untuk Katalog Kontrol Kepatuhan Komputasi Awan Jerman (C5) • Praktik Terbaik Operasional untuk IRS 1075 Paket kesesuaian berikut diperbarui: • AWS Paket Kesesuaian Control Tower Detective Guardrails • Praktik Terbaik Operasional untuk CISA Cyber Hal-hal Penting • Praktik Terbaik Operasional untuk Panduan Keamanan Siber ENISA untuk SMEs • Praktik Terbaik Operasional untuk FDA Judul 21 CFR Bagian 11 • Praktik Terbaik Operasional untuk FedRAMP (Sedang) • Praktik Terbaik Operasional untuk Keamanan HIPAA • Praktik Terbaik Operasional untuk Kerangka Privasi NIST v1.0	31 Agustus 2022

	• Praktik Terbaik Operasional untuk NYDFS 23 • Praktik Terbaik Operasional untuk Kerangka Keamanan Cyber RBI untuk UCBs • Praktik Terbaik Operasional untuk RBI MD-ITF	
Memulai dengan AWS Config dan pembaruan Paket Kesesuaian Kustom	Dengan rilis ini, AWS Config perbarui halaman Memulai AWS Config dan Menyiapkan AWS Config dengan Konsol, memperkenalkan halaman penyiapan 1-klik dan pengaturan Manual. AWS Config juga memperbarui halaman Paket Kesesuaian Kustom dengan panduan tentang cara membuat file YAMAL paket kesesuaian dari awal.	Agustus 25, 2022

AWS Systems Manager Dokumen (dokumen SSM) Integrasi dengan Paket Kesesuaian	Dengan rilis ini, Anda dapat membuat template paket kesesuaian dengan dokumen SSM. Untuk informasi selengkapnya tentang dokumen SSM, lihat AWS Systems Manager Dokumen di Panduan AWS Systems Manager Pengguna. Tipe data berikut diperbarui: • PutConformancePack • ConformancePackDetail • SSMDocumentDetail Template Halaman-halaman berikut dalam panduan pengembang diperbarui: • Menerapkan Paket Kesesuaian Menggunakan Konsol AWS Config • Menyebarkan Paket Kesesuaian Menggunakan Antarmuka Baris Perintah AWS	Agustus 24, 2022

Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` Kebijakan dan `AWS_ConfigRole` kebijakan sekarang memberikan izin tambahan untuk Amazon Simple Email Service (Amazon SES) AWS DataSync,, dan. AWS Cloud Map Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	22 Agustus 2022
AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke jenis sumber daya Amazon Athena, Amazon Detective, Amazon SageMaker AI, Amazon Route 53 AWS Database Migration Service ,AWS DMS(), AWS Glue, AWS Key Management Service AWS KMS(), dan Amazon Simple Email Service (Amazon SES). Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	Agustus 16, 2022

AWS Config mendukung paket kesesuaian baru	Dengan rilis ini, AWS Config update paket kesesuaian berikut: • Praktik Terbaik Operasional untuk NIST 1800 25 • Praktik Terbaik Operasional untuk NIST 800 181 • Praktik Terbaik Operasional untuk Beban Kerja Standar ABS CCIG 2.0 • Praktik Terbaik Operasional untuk Beban Kerja Material ABS CCIG 2.0 • Praktik Terbaik Operasional untuk ACSC Essential 8 • Praktik Terbaik Operasional untuk ACSC ISM • Praktik Terbaik Operasional untuk APRA CPG 234 • Praktik Terbaik Operasional untuk Tolok Ukur AWS Yayasan CIS v1.4 Level 1 • Praktik Terbaik Operasional untuk Tolok Ukur AWS Yayasan CIS v1.4 Level 2 • Praktik Terbaik Operasional untuk BNM T RMi • Praktik Terbaik Operasional untuk NIST CSF	1 Agustus 2022

Skor kepatuhan untuk paket kesesuaian	Dengan rilis ini, AWS Config memperkenalkan skor kepatuhan untuk paket kesesuaian, yang memberi Anda tampilan tingkat tinggi tentang status kepatuhan paket kesesuaian Anda. Anda dapat menggunak annya untuk mengidentifikasi, menyelidiki, dan memahami tingkat kepatuhan dalam paket kesesuaian Anda. Skor kepatuhan adalah persentase dari jumlah kombinasi aturan-sumber daya yang sesuai dalam paket kesesuaian dibandingkan dengan jumlah total kemungkinan kombinasi aturan-sumber daya dalam paket kesesuaian. Tipe data berikut diperbarui: • ListConformancePackComplianceScores • ConformancePackComplianceScore Halaman-halaman berikut dalam panduan pengembang diperbarui: • Melihat AWS Config Dashboard • Melihat Data Kepatuhan di Dasbor Paket Kesesuaian	26 Juli 2022

	• Mengelola Paket Kesesuaian (API)	
Pembaruan IAM keamanan	`ConfigConformsServiceRolePolicy` Kebijakan tersebut sekarang memberikan izin untuk mempublikasikan titik data metrik ke Amazon CloudWatch. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	25 Juli 2022

Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` `AWS_ConfigRole` Kebijakan dan kebijakan sekarang memberikan izin tambahan untuk Amazon Elastic Container Service (Amazon ECS), Amazon, Amazon, Amazon, Amazon, ElastiCache Amazon Managed Service untuk Apache Flink FSx, EventBridge Amazon Location Service, Amazon Managed Streaming untuk Apache Kafka, Amazon, Amazon Rekognition,, Amazon QuickSight Simple Storage Service (Amazon S3)) Simple Storage S3) AWS RoboMaker, Layanan Email Sederhana Amazon (Amazon SES),,,,, ,, (Pusat Identitas IAM AWS Amplify) AWS AppConfig, AWS AppSync AWS Billing Conductor AWS DataSync AWS Firewall Manager AWS Glue AWS IAM Identity Center EC2 Image Builder, dan Elastic Load Balancing. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	15 Juli 2022

AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke jenis sumber daya Amazon Elastic Compute Cloud (Amazon EC2) yang baru. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	8 Juli 2022
AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke jenis AWS Global Accelerator sumber daya baru. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	Juli 5, 2022
AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • autoscaling-launch-template • ecs-task-definition-log-konfigurasi • ecs-awsvpc-networking-enabled	1 Juli 2022

AWS Config mendukung paket kesesuaian baru	Dengan rilis ini, AWS Config mendukung paket kesesuaian berikut: • Praktik Terbaik Operasional untuk Profil Kontrol Cloud Sedang Pusat Keamanan Siber Kanada (CCCS) • Praktik Terbaik Operasional untuk Gramm Leach Bliley Act (GLBA) • Praktik Terbaik Operasional untuk GxP EU Annex 11 • Praktik Terbaik Keamanan untuk Amazon Elastic Kubernetes Service (Amazon EKS) • Praktik Terbaik Keamanan untuk Amazon Relational Database Service (Amazon RDS) • Praktik Terbaik Keamanan untuk AWS Lambda Paket kesesuaian berikut diperbarui: • Praktik Terbaik Operasional untuk AI dan ML • Praktik Terbaik Operasional untuk Amazon DynamoDB • Praktik Terbaik Operasional untuk Kontrol Keamanan Kritis CIS v8 IG1	30 Juni 2022

	• Praktik Terbaik Operasional untuk Kontrol Keamanan Kritis CIS v8 IG2 • Praktik Terbaik Operasional untuk Kontrol Keamanan Kritis CIS v8 IG3 • Praktik Terbaik Operasional untuk Keamanan HIPAA • Praktik Terbaik Operasional untuk NIST 800-53 rev 5 • Praktik Terbaik Operasional untuk NIST CSF	
AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke jenis sumber daya Amazon SageMaker AI baru. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	Juni 29, 2022

AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke Amazon Managed Streaming baru untuk Apache Kafka Kafka (Amazon MSK), Amazon Route 53 WorkSpaces, Amazon,, (IAM Access AWS Database Migration Service Analyzer AWS DMS), (),, AWS Step Functions dan jenis sumber daya Elastic Load Balancing. AWS Batch AWS Identity and Access Management Access Analyzer Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	14 Juni 2022

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • aurora-last-backup-recovery-point-dibuat • dynamodb-last-backup-recovery-point-dibuat • ebs-last-backup-recovery-point-dibuat • ec2- -dibuat last-backup-recovery-point • efs-last-backup-recovery-point-dibuat • fsx-last-backup-recovery-point-dibuat • rds-last-backup-recovery-point-dibuat • s3- -dibuat last-backup-recovery-point • storagegateway-last-backup-recovery-point-dibuat • virtualmachine-last-backup-recovery-point-dibuat	Juni 13, 2022

AWS Config Integrasi dengan AWS Security Hub	Dengan rilis ini, Anda dapat melihat hasil evaluasi aturan AWS Config terkelola dan kustom sebagai temuan di AWS Security Hub. Security Hub mengubah evaluasi aturan menjadi temuan, yang memberikan informasi lebih lanjut tentang sumber daya yang terkena dampak, seperti Nama Sumber Daya Amazon (ARN) dan tanggal pembuatan . Temuan ini dapat dilihat bersama temuan Security Hub lainnya, memberikan gambaran menyeluruh tentang postur keamanan Anda. Untuk informasi selengkapnya, lihat Mengirim Evaluasi Aturan ke Security Hub	7 Juni 2022

Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` Kebijakan dan `AWS_ConfigRole` kebijakan sekarang memberikan izin tambahan untuk Amazon Athena, Amazon Detective , Amazon, Amazon Macie, GuardDuty Amazon Simple Email Service (Amazon AWS Glue SES),, (), dan. AWS Resource Access Manager AWS RAM AWS IAM Identity Center Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	31 Mei 2022

AWS Config mendukung paket kesesuaian baru	Dengan rilis ini, AWS Config mendukung paket kesesuaian berikut: • Praktik Terbaik Keamanan untuk Amazon Elastic Container Service (Amazon ECS) • Praktik Terbaik Keamanan untuk Amazon Elastic File System (Amazon EFS) • Praktik Terbaik Keamanan untuk Amazon CloudFront • Praktik Terbaik Keamanan untuk AWS Auto Scaling • Praktik Terbaik Keamanan untuk AWS Network Firewall • Praktik Terbaik Keamanan untuk AWS Secrets Manager	31 Mei 2022
AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke Amazon SageMaker AI dan jenis AWS Step Functions sumber daya baru. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	26 Mei 2022
AWS Config mendukung paket kesesuaian baru	Dengan rilis ini, AWS Config update paket kesesuaian Praktik Terbaik Operasional untuk NERC CIP BCSI.	Mei 20, 2022

Komponen AWS Config Aturan	Dengan rilis ini, AWS Config memperkenalkan Komponen halaman AWS Config Aturan. Halaman ini membahas struktur definisi aturan, metadata aturan, dan praktik terbaik tentang cara menulis aturan dengan Python menggunakan AWS Config Rules Development Kit (RDK) dan AWS Config Rules Development Kit Library (). RDKlib	9 Mei 2022
Batas layanan meningkat untuk paket kesesuaian organisasi	Dengan rilis ini, AWS Config mendukung 180 AWS Config aturan per akun di semua paket kesesuaian organisasi. Untuk informasi selengkapnya, lihat Batas Layanan.	6 Mei 2022
AWS Config mendukung paket kesesuaian baru	Dengan rilis ini, AWS Config mendukung paket kesesuaian berikut: • Praktik Terbaik Keamanan untuk OpenSearch Layanan Amazon • Praktik Terbaik Keamanan untuk Amazon Redshift • Praktik Terbaik Keamanan untuk AWS CloudTrail • Praktik Terbaik Keamanan untuk AWS CodeBuild • Praktik Terbaik Keamanan untuk AWS WAF	29 April 2022

AWS Config pembaruan aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola s3- resources-protected-by-backup -plan.	April 11, 2022
Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` `AWS_ConfigRole` Kebijakan dan kebijakan sekarang memberikan izin tambahan untuk mendapatkan informasi tentang semua atau penyimpanan data AWS CloudTrail peristiwa tertentu (EDS), mendapatkan informasi tentang semua atau AWS CloudFormation sumber daya tertentu, mendapatkan daftar grup parameter DynamoDB Accelerator (DAX) atau grup subnet, mendapatkan informasi AWS Database Migration Service tentang AWS DMS() tugas replikasi untuk akun Anda di wilayah saat ini yang sedang diakses, dan dapatkan daftar semua kebijakan dalam tipe tertentu. AWS Organizations Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	7 April 2022

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • alb-desync-mode-check • autoscaling-capacity-rebalancing • autoscaling-launchconfig-requires-imdsv2 • autoscaling-launch-config-hop-batas • autoscaling-multiple-instance-types • clb-desync-mode-check • ecs-container-insights-enabled • ecs-fargate-latest-platform-versi • netfw-policy-default-action-fragmen-paket • netfw-policy-default-action-paket penuh • netfw-policy-rule-group-terkait • redshift-audit-logging-enabled • s3- lifecycle-policy-check • waf-regional-rule-not-kosong • waf-regional-rulegroup-not-kosong • waf-regional-webacl-not-kosong	4 April 2022

- vpc-peering-dns-resolution-periksa

AWS Config Aturan Kebijakan Kustom	Dengan rilis ini, AWS Config Anda dapat membuat aturan Kebijakan AWS Config Kustom menggunakan AWS CloudFormation Guard (guard). Guard adalah policy-as-code bahasa yang memungkinkan Anda menulis kebijakan yang diberlaku kan AWS Config tanpa perlu membuat fungsi Lambda untuk mengelola aturan kustom Anda. Aturan yang ditulis menggunakan kebijakan Guard dapat dibuat dari AWS Config konsol atau dengan menggunakan AWS Config aturan APIs. Halaman-halaman berikut dalam panduan pengembang diperbarui: • AWS Config Aturan Kustom • Membuat Aturan AWS Config Kustom dengan Guard Tipe data berikut diperbarui: • Sumber • CustomPolicyDetails • ConfigRuleEvaluationStatus • GetCustomRulePolicy • GetOrganizationCus tomRulePolicy	4 April 2022

	• OrganizationCustomPolicyRuleMetadata	
AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke jenis SecurityConfiguration sumber daya Amazon EMR yang baru. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	31 Maret 2022
AWS Config pembaruan aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola virtualmachine-resources-protected-by-backup-plan.	29 Maret 2022

AWS Config Integrasi dengan Amazon CloudWatch Metrics	Dengan rilis ini, AWS Config sekarang mendukung pelacakan AWS Config penggunaan dan metrik keberhasilan Anda dengan Amazon CloudWatch di halaman AWS Config Dasbor. CloudWatch metrik adalah layanan pemantaua n yang menyediakan data tentang kinerja sistem Anda, termasuk kemampuan untuk mencari, membuat grafik, dan membangun alarm pada metrik tentang sumber daya. AWS Dari AWS Config Dasbor, Anda dapat melihat lalu lintas apa yang mendorong AWS Config penggunaan dan metrik kunci untuk kegagalan yang terjadi dalam alur kerja Anda. Halaman berikut diperbarui: • Melihat AWS Config Dashboard	29 Maret 2022
AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke jenis sumber daya Amazon GuardDuty Detector baru. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	24 Maret 2022

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • clb-multiple-az • cloudfront-no-deprecated-ssl-protokol • cloudfront-traffic-to-origin-dienkripsi • cloudwatch-alarm-action-enabled-periksa • ec2- no-amazon-key-pair • ec2- paravirtual-instance-check • ec2- token-hop-limit-check • ec2- transit-gateway-auto-vpc -lampiran-dinonaktifkan • ecr-private-lifecycle-policy-dikonfigurasi • efs-access-point-enforce-root-direktori • efs-access-point-enforce-identitas pengguna • elbv2-multiple-az • kinesis-stream-encrypted • redshift-default-db-name-periksa • s3- event-notifications-enabled • sns-topic-message-delivery-notifikasi-diaktifkan • waf-global-rulegroup-not-kosong	Maret 23, 2022

	• waf-global-rule-not-kosong	
AWS Config mendukung paket kesesuaian baru	Dengan rilis ini, AWS Config update paket kesesuaian berikut: • Praktik Terbaik Operasional untuk Kontrol Keamanan Kritis CIS v8 IG1 • Praktik Terbaik Operasional untuk Kontrol Keamanan Kritis CIS v8 IG2 • Praktik Terbaik Operasional untuk Kontrol Keamanan Kritis CIS v8 IG3 • Praktik Terbaik Operasional untuk Pilar Keamanan AWS Kerangka Well-Architected • Praktik Terbaik Operasional untuk Esquema Nacional de Seguridad (ENS) Rendah • Praktik Terbaik Operasional untuk Medium Esquema Nacional de Seguridad (ENS) • Praktik Terbaik Operasional untuk Esquema Nacional de Seguridad (ENS) High • Praktik Terbaik Operasional untuk Pemberitahuan MAS 655 • Praktik Terbaik Operasional untuk NIST 1800-25	16 Maret 2022

Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` Kebijakan dan `AWS_ConfigRole` kebijakan sekarang memberikan izin tambahan untuk AWS CloudFormation. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	Maret 14, 2022
AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config memperbarui aturan terkelola berikut: • aurora-resources-protected-by-rencana cadangan • dynamodb-resources-protected-by-rencana cadangan • ebs-resources-protected-by-rencana cadangan • ec2- -rencana resources-protected-by-backup • efs-resources-protected-by-rencana cadangan • fsx-resources-protected-by-rencana cadangan • rds-resources-protected-by-rencana cadangan	10 Maret 2022

AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke jenis sumber daya Publik Amazon Elastic Container Registry yang baru. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	4 Maret 2022
AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke jenis sumber daya Amazon Elastic Compute Cloud yang baru. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	28 Februari 2022
AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • codedeploy-auto-rollback-monitor-diaktifkan • codedeploy-ec2- minimum-healthy-hosts-configured • codedeploy-lambda-allatonce-traffic-shift-dinonaktifkan	25 Februari 2022

Pencatatan dan Pemantauan dalam AWS Config Pembaruan	Dengan rilis ini, AWS Config update halaman Monitoring AWS Config with Amazon EventBridge Events untuk menggantikan referensi ke Amazon CloudWatch Events. Amazon EventBridge adalah cara yang lebih disukai untuk mengelola acara Anda. CloudWatch Acara dan EventBridge merupakan layanan dan API dasar yang sama, tetapi EventBridge menyediakan lebih banyak fitur. Perubahan yang Anda buat di salah satu CloudWatch atau EventBridge akan muncul di setiap konsol. Untuk informasi lebih lanjut, lihat Amazon. EventBridge	Februari 24, 2022
AWS Halaman SDK untuk AWS Config	Dengan rilis ini, AWS Config memperkenalkan halaman Menggunakan AWS Config dengan AWS SDK. AWS kit pengembangan perangkat lunak (SDKs) tersedia untuk banyak bahasa pemrograman populer. Setiap SDK menyediakan API, contoh kode, dan dokumentasi yang memudahkan developer untuk membangun aplikasi dalam bahasa pilihan mereka.	Februari 24, 2022

Pembaruan kebijakan Keamanan IAM Role Trust	Dengan rilis ini, AWS Config memperbarui pernyataan kebijakan kepercayaan IAM untuk memasukkan perlindungan keamanan dalam kebijakan kepercayaan yang membatasi akses `sourceARN` and/or `sourceAccountId` untuk operasi AWS Security Token Service ()AWS STS. Ini membantu memastikan bahwa kebijakan kepercayaan peran IAM mengakses sumber daya Anda hanya atas nama pengguna dan skenario yang diharapkan. Halaman berikut diperbarui: • Menambahkan Kebijakan Kepercayaan IAM ke Peran Anda	18 Februari 2022

Perubahan pada Rekaman Jenis Sumber Daya Global	AWS Config sekarang mengubah cara jenis sumber daya global baru direkam dalam AWS Config Perekaman. Jenis sumber daya global adalah AWS sumber daya yang tidak mengharuskan Anda menentukan wilayah saat pembuatan. Sebelum perubahan ini, Anda dapat mengaktifkan perekaman jenis sumber daya global di semua wilayah yang didukung di AWS Config. Setelah perubahan ini, jenis sumber daya global baru yang dimasukkan ke dalam AWS Config rekaman hanya dapat direkam di wilayah asal layanan untuk partisi komersial, dan AWS GovCloud (AS-Barat) untuk partisi. AWS GovCloud (US) Anda sekarang akan dapat melihat item konfigurasi untuk jenis sumber daya global baru ini hanya di wilayah asal mereka dan AWS GovCloud (AS-Barat). Untuk daftar wilayah asal untuk jenis sumber daya global yang dionboard setelah Februari 2022, lihat tabel di halaman Merekam Semua Jenis Sumber Daya yang Didukung.	18 Februari 2022

Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` Kebijakan dan `AWS_ConfigRole` kebijakan sekarang memberikan izin untuk mendapatkan detail tentang lingkungan Elastic Beanstalk dan deskripsi setelan untuk set konfigurasi Elastic Beanstalk yang ditentukan, mendapatkan peta atau versi Elasticsearch, menjelaskan grup opsi Amazon RDS yang tersedia untuk database, dan mendapatkan informasi OpenSearch tentang konfigurasi penerapan. CodeDeploy Kebijakan ini juga sekarang memberikan izin untuk mengambil kontak alternatif tertentu yang dilampirkan pada Akun AWS, mengambil informasi tentang kebijakan, mengambil AWS Organizations kebijakan repositori Amazon ECR, mengambil informasi tentang aturan yang AWS Config diarsipkan, mengambil daftar keluarga definisi tugas Amazon ECS, mencantumkan OUs unit organisasi root atau induk () dari OU atau akun turunan yang ditentukan, dan daftar kebijakan yang dilampirkan ke root target, unit organisas	Februari 10, 2022

i, atau akun yang ditentukan. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • autoscaling-multiple-az • codebuild-project-artifact-encryption • codebuild-project-environment-privileged-periksa • codebuild-project-logging-enabled • codebuild-project-s3-log-terenkripsi • ec2- security-group-attached-to -eni-periodik • ecr-private-image-scanning-diaktifkan • ecr-private-tag-immutability-diaktifkan • ecs-containers-nonprivileged • ecs-containers-readonly-access • ecs-no-environment-secrets • ecs-task-definition-memory-batas-keras • ecs-task-definition-nonroot-pengguna • ecs-task-definition-pid-mode-periksa • eks-cluster-oldest-supported-versi	Februari 10, 2022

	• eks-cluster-supported-version • lambda-vpc-multi-az-periksa • nacl-no-unrestricted-ssh-rdp • netfw-stateless-rule-group-tidak-kosong • rds-cluster-default-admin-periksa • rds-db-security-group-tidak diizinkan • rds-instance-default-admin-periksa • redshift-default-admin-check • s3- bucket-acl-prohibited • s3- version-lifecycle-policy-check • waf-global-webacl-not-kosong	
Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` Kebijakan dan `AWS_ConfigRole` kebijakan sekarang memberikan izin untuk membuat grup dan aliran CloudWatch log Amazon dan menulis log ke aliran log yang dibuat. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	2 Februari 2022

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • opensearch-access-control-enabled • opensearch-audit-logging-enabled • opensearch-data-node-fault-toleransi • opensearch-encrypted-at-rest • opensearch-https-required • opensearch-in-vpc-only • opensearch-logs-to-cloudwatch • opensearch-node-to-node-pemeriksaan enkripsi-	Januari 31, 2022
AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi pada jenis AWS CodeDeploy sumber daya. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	5 Januari 2022

AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke jenis sumber daya Amazon SageMaker AI baru. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	Desember 20, 2021
AWS Config mendukung paket kesesuaian baru	Dengan rilis ini, AWS Config mendukung paket kesesuaian berikut: • Praktik Terbaik Operasional untuk Panduan Keamanan Siber ENISA untuk SMEs	Desember 20, 2021
AWS Config mendukung paket kesesuaian baru	Dengan rilis ini, AWS Config mendukung paket kesesuaian berikut: • Praktik Terbaik Operasional untuk NIST 800 172 • Praktik Terbaik Operasional untuk NIST 800 181 Paket kesesuaian berikut diperbarui: • Praktik Terbaik Operasional untuk K-ISMS	18 November 2021

AWS Config mendukung paket kesesuaian baru	Dengan rilis ini, AWS Config mendukung paket kesesuaian berikut: • Praktik Terbaik Operasional untuk Amazon API Gateway • Praktik Terbaik Operasional untuk AWS Backup • Praktik Terbaik Operasional untuk CISA Cyber Hal-hal Penting • Praktik Terbaik Operasional untuk DevOps • Praktik Terbaik Operasional untuk Kerangka Privasi NIST v1.0 Paket kesesuaian berikut diperbarui: • Praktik Terbaik Operasional untuk FedRAMP (Rendah) • Praktik Terbaik Operasional untuk FedRAMP (Sedang)	29 Oktober 2021
AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke jenis sumber daya Amazon OpenSearch Service baru. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	Oktober 12, 2021

AWS Config mendukung paket kesesuaian baru	Dengan rilis ini, AWS Config update paket kesesuaian berikut: • Praktik Terbaik Operasional untuk MAS TRMG	Oktober 12, 2021

AWS Config mendukung paket kesesuaian baru	Dengan rilis ini, AWS Config update paket kesesuaian berikut: • Praktik Terbaik Operasional untuk Beban Kerja Material ABS CCIG 2.0 • Praktik Terbaik Operasional untuk Beban Kerja Standar ABS CCIG 2.0 • Praktik Terbaik Operasional untuk ACSC Essential 8 • Praktik Terbaik Operasional untuk ACSC ISM • Praktik Terbaik Operasional untuk BNM T RMi • Praktik Terbaik Operasional untuk CMMC Level 1 • Praktik Terbaik Operasional untuk CMMC Level 2 • Praktik Terbaik Operasional untuk CMMC Level 3 • Praktik Terbaik Operasional untuk CMMC Level 4 • Praktik Terbaik Operasional untuk CMMC Level 5 • Praktik Terbaik Operasional untuk FDA Judul 21 CFR Bagian 11 • Praktik Terbaik Operasional untuk FFIEC • Praktik Terbaik Operasional untuk Pemberitahuan MAS 655	30 September 2021

	• Praktik Terbaik Operasional untuk NBC TRMG • Praktik Terbaik Operasional untuk NERC CIP • Praktik Terbaik Operasional untuk NIST 800-53 rev 5	
Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` Kebijakan dan `AWS_ConfigRole` kebijakan sekarang memberikan izin untuk mendapatkan detail tentang OpenSearch Layanan Amazon (OpenSearch Layanan) domain/domains dan untuk mendapatkan daftar parameter terperinci untuk grup parameter DB Amazon Relational Database Service (Amazon RDS) tertentu. Kebijakan ini juga memberikan izin untuk mendapatkan detail tentang ElastiCache snapshot Amazon. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	8 September 2021

AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke jenis sumber daya Amazon Elastic Compute Cloud yang baru. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	7 September 2021

AWS Config mendukung paket kesesuaian baru	Dengan rilis ini, AWS Config update paket kesesuaian berikut: • Praktik Terbaik Operasional untuk APRA CPG 234 • Praktik Terbaik Operasional untuk Tolok Ukur AWS Yayasan CIS v1.4 Level 1 • Praktik Terbaik Operasional untuk Tolok Ukur AWS Yayasan CIS v1.4 Level 2 • Praktik Terbaik Operasional untuk Prinsip Keamanan Cloud NCSC • Praktik Terbaik Operasional untuk Kerangka Penilaian Cyber NCSC • Praktik Terbaik Operasional untuk NIST 800 171 • Praktik Terbaik Operasional untuk NIST CSF • Praktik Terbaik Operasional untuk Kerangka Keamanan Cyber RBI untuk UCBs • Praktik Terbaik Operasional untuk RBI MD-ITF • Praktik Terbaik Operasional untuk NYDFS 23 • Praktik Terbaik Operasional untuk PCI DSS 3.2.1	Agustus 30, 2021

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • aurora-resources-protected-by-rencana cadangan • backup-plan-min-frequency-and-min-retention-check • backup-recovery-point-encrypted • backup-recovery-point-manual-penghapusan-dinonaktifkan • backup-recovery-point-minimum-pemeriksaan retensi • dynamodb-resources-protected-by-rencana cadangan • ebs-resources-protected-by-rencana cadangan • ec2- -rencana resources-protected-by-backup • efs-resources-protected-by-rencana cadangan • fsx-resources-protected-by-rencana cadangan • rds-resources-protected-by-rencana cadangan	Agustus 20, 2021

AWS Config mendukung paket kesesuaian baru	Dengan rilis ini, AWS Config mendukung paket kesesuaian berikut: • Praktik Terbaik Operasional untuk NZISM	Agustus 20, 2021
Keamanan pembaruan kebijakan Amazon SNS	Dengan rilis ini, AWS Config memperbarui pernyataan kebijakan IAM untuk topik Amazon SNS saat menggunakan peran terkait layanan untuk menyertakan perlindungan keamanan yang membatasi akses dalam kebijakan topik. `sourceARN` and/or `sourceAccountId` Ini membantu memastikan Amazon SNS mengakses sumber daya Anda hanya atas nama pengguna dan skenario yang diharapkan. Halaman berikut diperbarui: • Izin untuk Topik Amazon SNS	17 Agustus 2021

Pembaruan AWS Lambda kebijakan keamanan	Dengan rilis ini, AWS Config memperbarui kebijakan AWS Lambda berbasis sumber daya untuk aturan AWS Config khusus untuk menyertak an perlindungan keamanan yang membatasi akses dalam permintaan pemanggil an. `sourceARN` and/or `sourceAccountId` Ini membantu memastikan AWS Lambda mengakses sumber daya Anda hanya atas nama pengguna dan skenario yang diharapkan. Halaman-halaman berikut diperbarui: • AWS::Config::ConfigRule • Mengembangkan Aturan Kustom untuk AWS Config	Agustus 12, 2021
AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke jenis sumber daya Amazon Kinesis. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	6 Agustus 2021

AWS Config mendukung paket kesesuaian baru	Dengan rilis ini, AWS Config mendukung paket kesesuaian berikut: • Praktik Terbaik Operasional untuk Esquema Nacional de Seguridad (ENS) High Paket kesesuaian berikut diperbarui: • Praktik Terbaik Operasional untuk Pilar Keandalan AWS Kerangka Kerja yang Dirancang dengan Baik • Praktik Terbaik Operasional untuk Pilar Keamanan AWS Kerangka Well-Architected • Praktik Terbaik Operasional untuk Esquema Nacional de Seguridad (ENS) Rendah • Praktik Terbaik Operasional untuk Medium Esquema Nacional de Seguridad (ENS) • Praktik Terbaik Operasional untuk Keamanan HIPAA	30 Juli 2021
Contoh AWS Lambda Fungsi untuk Aturan AWS Config Kustom	Dengan rilis ini, AWS Config menyediakan contoh fungsi Python di Example AWS Lambda Functions for AWS Config Rules (Python).	29 Juli 2021

Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` Kebijakan dan `AWS_ConfigRole` kebijakan sekarang memberikan izin untuk mencantumkan tag untuk grup log, tag daftar untuk mesin status, dan daftar semua mesin status. Kebijakan ini sekarang memberikan izin untuk mendapatkan detail tentang mesin negara. Kebijakan ini juga sekarang mendukung izin tambahan untuk Amazon EC2 Systems Manager (SSM), Amazon Elastic Container Registry, Amazon FSx, Amazon Data Firehose, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Relational Database Service (Amazon RDS), Amazon Route 53 SageMaker , Amazon AI, Layanan Pemberitahuan Sederhana Amazon,,, dan. AWS Database Migration Service AWS Global Accelerator AWS Storage Gateway Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	28 Juli 2021

AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi pada jenis AWS Backup sumber daya. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	14 Juli 2021
AWS Config mendukung paket kesesuaian baru	Dengan rilis ini, AWS Config mendukung paket kesesuaian berikut: • Praktik Terbaik Operasional untuk Kontrol Keamanan Kritis CIS v8 IG1 • Praktik Terbaik Operasional untuk Kontrol Keamanan Kritis CIS v8 IG2 • Praktik Terbaik Operasional untuk Kontrol Keamanan Kritis CIS v8 IG3 • Praktik Terbaik Operasional untuk NIST 1800 25	Juli 9, 2021
AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • ssm-document-not-public • s3- account-level-public-access -blok-periodik	25 Juni 2021

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • ec2- instance-multiple-eni-check • elbv2- acm-certificate-required • autoscaling-launch-config-public-ip-dinonaktifkan	10 Juni 2021

Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` Kebijakan dan `AWS_ConfigRole` kebijakan sekarang memberikan izin untuk melihat izin AWS Systems Manager dokumen dan informasi tentang IAM Access Analyzer. Kebijakan ini sekarang mendukung jenis AWS sumber daya tambahan untuk Amazon Kinesis, Amazon, Amazon EMR, ElastiCache Amazon Route 53, dan AWS Network Firewall Amazon Relational Database Service (Amazon RDS). Perubahan izin ini memungkinkan AWS Config untuk memanggil read-only yang APIs diperlukan untuk mendukung jenis sumber daya ini. Kebijakan ini juga sekarang mendukung pemfilteran fungsi Lambda @Edge untuk aturan terkelola lambda-inside-vpc AWS Config . Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	8 Juni 2021

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • elasticsearch-logs-to-cloudwatch • rds-cluster-multi-az-diaktifkan • api-gw-associated-with-waf • iam-policy-no-statements-with-full-access	19 Mei 2021
AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke jenis sumber daya Amazon Elastic File System. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	13 Mei 2021

Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` Kebijakan dan `AWS_ConfigRole` kebijakan sekarang memberikan izin yang memungkinkan AWS Config untuk melakukan panggilan GET hanya-baca ke API Gateway guna mendukung Aturan Konfigurasi untuk API Gateway. Kebijakan ini juga menambahkan izin yang memungkinkan AWS Config untuk memanggil Amazon Simple Storage Service (Amazon S3) APIs read-only, yang diperlukan untuk mendukung jenis sumber daya baru. `AWS::S3::AccessPoint` Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	10 Mei 2021
AWS Config Aturan Kustom	Halaman-halaman berikut dalam panduan pengembang diperbarui: • Memulai dengan Aturan Kustom untuk AWS Config • Mengembangkan Aturan Kustom untuk AWS Config	30 April 2021

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • aurora-mysql-backtracking-enabled • ec2- instance-profile-attached • ecs-task-definition-user-for-host-mode-check • no-unrestricted-route-to-igw • rds-automatic-minor-version-upgrade diaktifkan • redshift-enhanced-vpc-routing-diaktifkan	April 15, 2021

Pembaruan IAM keamanan	`AWSConfigServiceRolePolicy` Kebijakan dan `AWS_ConfigRole` kebijakan sekarang memberikan izin untuk melihat informasi tentang dokumen AWS Systems Manager tertentu. Kebijakan ini juga sekarang mendukung jenis AWS sumber daya tambahan untuk AWS Backup, Amazon Elastic File System, Amazon ElastiCache, Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud EC2 (Amazon), Amazon SageMaker Kinesis, Amazon AI, dan AWS Database Migration Service Amazon Route 53. Perubahan izin ini memungkinkan AWS Config untuk memanggil read-only yang APIs diperlukan untuk mendukung jenis sumber daya ini. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Config.	14 April 2021

Kepatuhan Paket Kesesuaian sebagai Item Konfigurasi () CIs	Dengan rilis ini, AWS Config mendukung kepatuhan paket kesesuaian sebagai item konfigurasi. Ini memungkinkan Anda untuk: • Lihat garis waktu perubahan status kepatuhan paket kesesuaian Anda • Kesesuaian agregat mengemas kepatuhan di beberapa akun dan wilayah • Gunakan kueri lanjutan untuk memeriksa kepatuhan paket kesesuaian Anda Tipe data berikut diperbarui: • DescribeAggregateComplianceByConformancePacks • GetAggregateConformancePackComplianceSummary Halaman-halaman berikut dalam panduan pengembang diperbarui: • Melihat Data Kepatuhan di Dasbor Paket Kesesuaian • Melihat Garis Waktu Riwayat Kepatuhan untuk Paket Kesesuaian	30 Maret 2021

	• Melihat Data Kepatuhan di Dasbor Agregator • Menanyakan Status Sumber Daya Konfigurasi Saat Ini AWS • Jenis Sumber Daya yang Didukung	
Pembaruan pagination	Dengan rilis ini, fitur kueri AWS Config lanjutan sekarang mendukung pagination untuk kueri yang berisi fungsi agregat, seperti COUNT dan SUM. Anda sekarang dapat menggunakan kueri lanjutan untuk mendapatkan hasil lengkap untuk kueri agregat Anda melalui pagination, yang sebelumnya dibatasi hingga 500 baris. Untuk informasi selengkapnya, lihat Menanyakan Status Sumber Daya Konfigurasi Saat Ini AWS	26 Maret 2021
Dukungan wilayah	Dengan rilis ini, AWS Config dan AWS Config Aturan sekarang didukung di Wilayah Asia Pasifik (Osaka).	4 Maret 2021

AWS Config mendukung jenis sumber daya baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke Amazon Elastic Container Registry, Amazon Elastic Container Service, dan jenis resource Amazon Elastic Kubernetes Service. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung.	25 Februari 2021
Dukungan enkripsi KMS	Dengan rilis ini, Anda AWS Config dapat menggunak an enkripsi berbasis KMS pada objek yang dikirimkan AWS Config untuk pengiriman bucket S3. Tipe data berikut diperbarui: • DeliveryChannel • PutDeliveryChannel Halaman-halaman berikut dalam panduan pengembang diperbarui: • Izin untuk Kunci KMS • Izin untuk Peran IAM Ditugaskan AWS Config	16 Februari 2021

AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • secretsmanager-secret-periodic-rotation • secretsmanager-secret-unused • secretsmanager-using-cmk	16 Februari 2021
Dukungan Wilayah Kueri Tersimpan	Dengan rilis ini, kueri yang disimpan sekarang didukung di Wilayah AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat).	15 Februari 2021
Dukungan wilayah agregasi data multi-akun multi-akun	Dengan rilis ini, agregasi data multi-wilayah multi-akun sekarang didukung di Wilayah Afrika (Cape Town) dan Eropa (Milan). Untuk informasi selengkapnya, lihat Agregasi Data Multi-Wilayah Multi-Akun.	15 Februari 2021
Kueri lanjutan Dukungan wilayah	Dengan rilis ini, kueri lanjutan sekarang didukung di Wilayah Afrika (Cape Town) dan Eropa (Milan). Untuk informasi selengkapnya, lihat Menanyakan Status AWS Sumber Daya Konfigurasi Saat Ini.	15 Februari 2021

AWS Config pemberitahuan riwayat dokumentasi tersedia melalui umpan RSS	Anda sekarang dapat menerima pemberitahuan tentang pembaruan AWS Config dokumentasi dengan berlangganan umpan RSS.	1 Januari 2021

Pembaruan Sebelumnya

Tabel berikut menjelaskan riwayat rilis dokumentasi AWS Config sebelum 31 Desember 2020.

Perubahan	Deskripsi	Tanggal Rilis
Dukungan Kueri Tersimpan	Dengan rilis ini, AWS Config memungkinkan Anda untuk menyimpan kueri Anda. Setelah Anda menyimpan kueri, Anda dapat mencarinya, menyalinnya ke editor kueri, mengeditnya, atau menghapus nya. Untuk informasi selengkapnya tentang cara menyimpan kueri, lihat Kueri Menggunakan Editor Kueri SQL untuk AWS Config (Konsol) danQuery Menggunakan SQL Query Editor untuk AWS Config ()AWS CLI. Untuk informasi selengkapnya APIs, lihat Referensi AWS Config API: • PutStoredQuery • GetStoredQuery • ListStoredQueries • DeleteStoredQuery Lihat juga Batas Layanan untuk AWS Config.	21 Desember 2020

Perubahan	Deskripsi	Tanggal Rilis
Dukungan pemeriksaan proses	Dengan rilis ini, AWS Config mendukung pemeriksaan proses yang merupakan jenis AWS Config aturan yang memungkinkan Anda melacak tugas eksternal dan internal yang memerlukan verifikasi sebagai bagian dari paket kesesuaian. Dengan pemeriksaan proses, Anda dapat membuat daftar kepatuhan persyaratan dan tindakan di satu lokasi. Untuk informasi selengkapnya tentang pemeriksaan proses, lihat AWS Config Memproses Pemeriksaan Dalam Paket Kesesuaian untuk AWS Config topik dan PutExternalEvaluationAPI.	17 Desember 2020

Perubahan	Deskripsi	Tanggal Rilis
AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • api-gw-ssl-enabled • api-gw-xray-enabled • beanstalk-enhanced-health-reporting-diaktifkan • cloudfront-accesslogs-enabled • cloudfront-associated-with-waf • cloudfront-custom-ssl-certificate • elastic-beanstalk-managed-updates-diaktifkan • rds-cluster-iam-authentication-diaktifkan • redshift-cluster-kms-enabled • s3- -dilarang bucket-level-public-access • subnet-auto-assign-public-ip-dinonaktifkan • vpc-network-acl-unused-periksa	17 Desember 2020
AWS Config mendukung AWS Network Firewall	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi pada jenis sumber daya Firewall AWS Network Firewall FirewallPolicy RuleGroup, dan Firewall Anda. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.	4 Desember 2020

Perubahan	Deskripsi	Tanggal Rilis
Pembaruan dokumentasi	AWS Config menambahkan dukungan untuk agregasi data sumber daya di seluruh organisasi dalam akun administrator yang didelegasikan. Sekarang Anda dapat menggunakan akun administrator yang didelegasikan untuk menggabungkan konfigurasi sumber daya dan data kepatuhan dari semua akun anggota organisasi AWS di Organizations. Untuk informasi lebih lanjut, lihat PutConfigurationAggregator, Membuat Agregator untuk AWS Config danMendaftarkan Administrator Delegasi untuk AWS Config.	4 Desember 2020
AWS Config mendukung paket kesesuaian baru	• Praktik Terbaik Operasional untuk Esquema Nacional de Seguridad (ENS) Rendah • Praktik Terbaik Operasional untuk Medium Esquema Nacional de Seguridad (ENS) • Praktik Terbaik Operasional untuk Kerangka Penilaian Cyber NCSC • Praktik Terbaik Operasional untuk Kerangka Keamanan Cyber RBI untuk UCBs	30 Oktober 2020

Perubahan	Deskripsi	Tanggal Rilis
AWS Config mendukung paket kesesuaian baru	• Praktik Terbaik Operasional untuk ACSC Essential 8 • Praktik Terbaik Operasional untuk ACSC ISM • Praktik Terbaik Operasional untuk AI dan ML • Praktik Terbaik Operasional untuk Manajemen Aset • Praktik Terbaik Operasional untuk BCP dan DR • Praktik Terbaik Operasional untuk EC2 • Praktik Terbaik Operasional untuk K-ISMS • Praktik Terbaik Operasional untuk Load Balancing • Praktik Terbaik Operasional untuk Penebangan • Praktik Terbaik Operasional untuk Pemantauan • Praktik Terbaik Operasional untuk Tanpa Server	22 Oktober 2020

Perubahan	Deskripsi	Tanggal Rilis
AWS Config mendukung paket kesesuaian baru	• Praktik Terbaik Operasional untuk APRA CPG 234 • Praktik Terbaik Operasional untuk FedRAMP (Rendah) • Praktik Terbaik Operasional untuk Pemberitahuan MAS 655 • Praktik Terbaik Operasional untuk NBC TRMG • Praktik Terbaik Operasional untuk Prinsip Keamanan Cloud NCSC • Praktik Terbaik Operasional untuk RBI MD-ITF	15 Oktober 2020

Perubahan	Deskripsi	Tanggal Rilis
AWS Config mendukung paket kesesuaian baru	• Praktik Terbaik Operasional untuk Beban Kerja Material ABS CCIG 2.0 • Praktik Terbaik Operasional untuk Beban Kerja Standar ABS CCIG 2.0 • Praktik Terbaik Operasional untuk BNM T RMi • Praktik Terbaik Operasional untuk Ketahanan Data • Praktik Terbaik Operasional untuk Data Lakes dan Layanan Analytics • Praktik Terbaik Operasional untuk Enkripsi dan Manajemen Kunci • Praktik Terbaik Operasional untuk FDA Judul 21 CFR Bagian 11 • Praktik Terbaik Operasional untuk Sumber Daya yang Dapat Diakses Publik • Praktik Terbaik Operasional untuk MAS TRMG • Praktik Terbaik Operasional untuk NERC CIP BCSI • Praktik Terbaik Operasional untuk NYDFS 23	8 Oktober 2020

Perubahan	Deskripsi	Tanggal Rilis
AWS Config mendukung paket kesesuaian baru	• Praktik Terbaik Operasional untuk Pilar Keandalan AWS Kerangka Well-Architected • Praktik Terbaik Operasional untuk Pilar Keamanan AWS Kerangka Well-Architected • Praktik Terbaik Operasional untuk Layanan Komputasi • Praktik Terbaik Operasional untuk Layanan Database • Praktik Terbaik Operasional untuk Layanan Manajemen dan Tata Kelola • Praktik Terbaik Operasional untuk Jaringan dan Layanan Pengiriman Konten • Praktik Terbaik Operasional untuk Layanan Keamanan, Identitas, dan Kepatuhan • Praktik Terbaik Operasional untuk Layanan Penyimpanan	26 Oktober 2020
AWS Config mendukung paket kesesuaian baru	• Praktik Terbaik Operasional untuk FedRAMP (Sedang) • Praktik Terbaik Operasional untuk FFIEC • Praktik Terbaik Operasional untuk Keamanan HIPAA • Praktik Terbaik Operasional untuk NIST 800-53 rev 4 • Praktik Terbaik Operasional untuk NIST 800 171	Senin, 28 September 2020

Perubahan	Deskripsi	Tanggal Rilis
Pembaruan dokumentasi	Topik paket kesesuaian berikut diperbarui. • Prasyarat untuk Paket Kesesuaian untuk AWS Config • Menyebarkan Paket Kesesuaian untuk AWS Config • Mengelola Paket Kesesuaian untuk Semua Akun AWS Config di Organisasi Anda	Senin, 28 September 2020
AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • iam-customer-policy-blocked-kms-tindakan • iam-inline-policy-blocked-kms-tindakan	17 September 2020
AWS Config mendukung AWS WAF v2	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke WebACL AWS WAF v2 IPSet,,,, RegexPatternSet RuleGroup , ManagedRuleSet dan jenis sumber daya Anda. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.	1 September 2020

Perubahan	Deskripsi	Tanggal Rilis
Pembaruan dokumentasi	Catatan telah ditambahkan Akses penuh ke AWS Config tentang membuat izin khusus yang memberikan akses penuh. Dokumentasi telah diperbarui untuk aturan berikut: • s3- -diaktifkan bucket-server-side-encryption • ec2- instance-detailed-monitoring-enabled • ec2- managedinstance-platform-check	24 Agustus 2020
Pembaruan dokumentasi	Praktik Terbaik Operasional untuk PCI DSS 3.2.1 dan Praktik Terbaik Operasional untuk NIST CSF template diperbarui.	14 Agustus 2020
Pembaruan dokumentasi	Contoh pertanyaan hubungan ditambahkan. Untuk informasi selengkapnya, lihat Contoh Pertanyaan Hubungan untuk AWS Config.	30 Juli 2020

Perubahan	Deskripsi	Tanggal Rilis
Pembaruan dokumentasi	Tipe data berikut diperbarui: • ConfigurationAggregator • RemediationConfiguration • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStatuses • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePackStatuses • GetOrganizationConformancePackDetailedStatus	23 Juli 2020
AWS Config mendukung jenis sumber daya AWS Systems Manager	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke tipe sumber daya data file AWS Systems Manager. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.	9 Juli 2020
Pembaruan dokumentasi	Praktik Terbaik Operasional untuk Manajemen AWS Identitas Dan Aksesdan Praktik Terbaik Operasional untuk PCI DSS 3.2.1 template diperbarui.	9 Juli 2020

Perubahan	Deskripsi	Tanggal Rilis
AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • account-part-of-organizations • alb-http-drop-invalid-header-diaktifkan • alb-waf-enabled • cloudfront-default-root-object-dikonfigurasi • cloudfront-origin-access-identity-diaktifkan • cloudfront-origin-failover-enabled • cloudfront-sni-enabled • cloudtrail-security-trail-enabled • cw-loggroup-retention-period-periksa • dax-encryption-enabled • dynamodb-in-backup-plan • ebs-in-backup-plan • ec2-imdsv2-periksa • efs-in-backup-plan • eks-endpoint-no-public-akses • eks-secrets-encrypted • elasticsearch-node-to-node-pemeriksaan enkripsi- • elb-cross-zone-load-menyeimbangkan diaktifkan • elb-tls-https-listeners-hanya • iam-no-inline-policy-periksa • rds-cluster-deletion-protection-diaktifkan	9 Juli 2020

Perubahan	Deskripsi	Tanggal Rilis
	• rds-in-backup-plan • rds-instance-deletion-protection-diaktifkan • rds-instance-iam-authentication-diaktifkan • rds-logging-enabled • redshift-backup-enabled • waf-classic-logging-enabled • wafv2-logging diaktifkan Untuk informasi selengkapnya, lihat Daftar Aturan AWS Config Terkelola.	
Dukungan wilayah agregasi data multi-akun multi-akun	Dengan rilis ini, agregasi data multi-wilayah multi-akun kini didukung di Wilayah Asia Pasifik (Hong Kong) dan Timur Tengah (Bahrain). Untuk informasi selengkapnya, lihat Multi-Account Multi-Region Data Aggregation dan Pemecahan Masalah untuk Agregasi Data Multi-Wilayah Multi-Akun untuk AWS Config.	1 Juli 2020
Kueri lanjutan Dukungan wilayah	Dengan rilis ini, kueri lanjutan sekarang didukung di Wilayah Asia Pasifik (Hong Kong) dan Timur Tengah (Bahrain). Untuk informasi selengkapnya, lihat Menanyakan Status Konfigurasi AWS Sumber Daya Saat Ini dengan AWS Config.	1 Juli 2020

Perubahan	Deskripsi	Tanggal Rilis
Pembaruan dokumentasi	Dokumentasi telah diperbarui untuk aturan berikut: • ec2- -periksa managedinstance-association-compliance-status • iam-policy-no-statements-with-admin-access • tag yang dibutuhkan • restricted-common-ports • rds-snapshots-public-prohibited • s3- bucket-policy-grantee-check	30 Juni 2020
Pembaruan dokumentasi	Dokumentasi telah diperbarui dengan informasi tentang keamanan untuk AWS Config. Lihat Keamanan di AWS Config.	24 Juni 2020
Pembaruan dokumentasi	AWS Control Tower Template Detective Guardrails Conformance Pack diperbarui. Untuk informasi selengkapnya, lihat AWS Paket Kesesuaian Pagar Pembatas Detektif Menara Kontrol.	4 Juni 2020
AWS Config mendukung paket kesesuaian baru	Dengan rilis ini, AWS Config mendukung Praktik Terbaik Operasional untuk paket kesesuaian CSF NIST. Untuk informasi selengkapnya, lihat Praktik Terbaik Operasional untuk NIST CSF .	29 Mei 2020

Perubahan	Deskripsi	Tanggal Rilis
AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • dynamodb-pitr-enabled • dynamodb-table-encrypted-kms • ec2- ebs-encryption-by-default • rds-snapshot-encrypted • redshift-require-tls-ssl • s3- bucket-default-lock-enabled • s3- default-encryption-kms • Securityhub-enabled • sns-encrypted-kms Untuk informasi selengkapnya, lihat Daftar Aturan AWS Config Terkelola.	28 Mei 2020

Perubahan	Deskripsi	Tanggal Rilis
Dukungan administrator yang didelegas ikan	Dengan rilis ini, Anda dapat menerapkan AWS Config aturan dan paket kesesuaian dari akun anggota yang didelegasikan di organisasi Anda, selain akun manajemen. Untuk informasi selengkapnya APIs, lihat Referensi AWS Config API: • PutOrganizationConfigRule • PutOrganizationConformancePack • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStatuses • DeleteOrganizationConfigRule • DeleteOrganizationConformancePack • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePackStatuses • GetOrganizationConformancePackDetailedStatus Untuk informasi selengkapnya, lihat Batas Layanan untuk AWS Config.	27 Mei 2020

Perubahan	Deskripsi	Tanggal Rilis
AWS Config aturan Dukungan wilayah	Dengan rilis ini, beberapa AWS Config aturan didukung di wilayah Afrika (Cape Town) dan Eropa (Milan). Untuk daftar rinci aturan dan wilayah tempat mereka didukung, lihatDaftar Aturan AWS Config Terkelola.	28 April 2020
AWS Config mendukung paket kesesuaian baru	Dengan rilis ini, AWS Config mendukung dua paket kesesuaian. • AWS Paket Kesesuaian Pagar Pembatas Detektif Menara Kontrol • Praktik Terbaik Operasional untuk CIS Untuk informasi selengkapnya, lihat Templat Contoh Paket Kesesuaian untuk AWS Config.	22 April 2020
AWS Config mendukung AWS Secrets Manager	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke rahasia Secrets Manager Anda. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.	20 April 2020

Perubahan	Deskripsi	Tanggal Rilis
AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • secretsmanager-rotation-enabled-check • secretsmanager-scheduled-rotation-success-periksa Untuk informasi selengkapnya, lihat Daftar Aturan AWS Config Terkelola.	16 April 2020
Paket kesesuaian Dukungan Wilayah	Dengan rilis ini, paket kesesuaian sekarang didukung di Asia Pasifik (Hong Kong) dan Timur Tengah (Bahrain). Untuk informasi selengkapnya, lihat Conformance Packs.	8 April 2020
Pembaruan dokumentasi	AWS Config batas tersedia dalam panduan pengembang ini. Untuk informasi selengkapnya, lihat Batas Layanan untuk AWS Config.	8 April 2020
Pembaruan dokumentasi	Sumber daya pihak ketiga yang dikelola (yaitu,created/updated/deleted) melalui AWS CloudFormation registri secara otomatis dilacak AWS Config sebagai item konfigurasi. Untuk informasi selengkapnya, lihat Merekam Konfigurasi dengan AWS Config Sumber Daya Pihak Ketiga menggunakan AWS CLI.	30 Maret 2020

Perubahan	Deskripsi	Tanggal Rilis
Pembaruan dokumentasi	Aturan AWS Config Terkelola diperbarui untuk menyertakan Wilayah AWS informasi. Untuk informasi selengkapnya, lihat Daftar Aturan AWS Config Terkelola.	27 Maret 2020
AWS Config mendukung jenis sumber daya Amazon SNS	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke topik Amazon SNS Anda. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.	6 Maret 2020
Dukungan wilayah agregasi data multi-akun multi-akun	Dengan rilis ini, agregasi data multi-wilayah multi-akun sekarang didukung di Wilayah Eropa (Stockholm). Untuk informasi selengkapnya, lihat Multi-Account Multi-Region Data Aggregation.	5 Maret 2020
Kueri lanjutan Dukungan wilayah	Dengan rilis ini, kueri lanjutan sekarang didukung di Wilayah Eropa (Stockholm). Untuk informasi selengkapnya, lihat Menanyakan Status Konfigurasi AWS Sumber Daya Saat Ini dengan AWS Config.	5 Maret 2020

Perubahan	Deskripsi	Tanggal Rilis
AWS Config memungkinkan Anda menjalankan kueri lanjutan dengan agregator konfigurasi	Dengan rilis ini, AWS Config menambahkan dukungan untuk menjalankan kueri lanjutan berdasarkan properti konfigurasi sumber daya dengan agregator konfigurasi, memungkinkan Anda menjalankan kueri yang sama di beberapa akun dan Wilayah. Untuk informasi selengkapnya, lihat Menanyakan Status Konfigurasi AWS Sumber Daya Saat Ini dengan AWS Config. Dengan rilis ini, AWS Config tambahkan `SelectAggregateResourceConfig` API. Untuk informasi selengkapnya, lihat SelectAggregateResourceConfigdi Referensi AWS Config API:	28 Februari 2020
AWS Config mendukung jenis sumber daya Amazon SQS	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi pada antrean Amazon SQS Anda. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.	13 Februari 2020

Perubahan	Deskripsi	Tanggal Rilis
AWS CloudFormation dukungan untuk paket Kesesuaian	Dengan rilis ini, AWS CloudFormation dukungan untuk sumber daya berikut ditambahkan: `AWS::Config::ConformancePack` dan`OrganizationConformancePack` . • AWS::Config::ConformancePack Gunakan `AWS::Config::ConformancePack` sumber daya untuk membuat Paket Kesesuaian yang merupakan kumpulan AWS Config aturan yang dapat dengan mudah digunakan di akun dan Wilayah dan di seluruh Organisasi. AWS • AWS::Config::OrganizationConformancePaket Gunakan `AWS::Config::OrganizationConformancePack` sumber daya untuk membuat Paket Kesesuaian Organisasi yang memiliki informasi tentang paket kesesuaian yang AWS Config dibuat di akun anggota.	13 Februari 2020

Perubahan	Deskripsi	Tanggal Rilis
AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • api-gw-execution-logging-diaktifkan • ec2-stopped-instance • elasticache-redis-cluster-automatic-backup-periksa • emr-master-no-public-ip • guardduty-non-archived-findings • rds-enhanced-monitoring-enabled • s3- -blok account-level-public-access • sagemaker-endpoint-configuration-kms-kunci-dikonfigurasi • service-vpc-endpoint-enabled Untuk informasi selengkapnya, lihat Daftar Aturan AWS Config Terkelola.	20 Desember 2019

Perubahan	Deskripsi	Tanggal Rilis
Rekam konfigurasi untuk jenis sumber daya khusus	Dengan rilis ini, AWS Config memperkenalkan dukungan untuk merekam konfigurasi untuk jenis sumber daya kustom. Anda dapat mempublikasikan data konfigurasi sumber daya pihak ketiga ke dalam AWS Config dan melihat serta memantau inventaris sumber daya dan riwayat konfigurasi menggunakan AWS Config konsol dan APIs. Untuk informasi selengkapnya, lihat Merekam Konfigurasi dengan AWS Config Sumber Daya Pihak Ketiga menggunakan AWS CLI. Untuk informasi selengkapnya APIs, lihat Referensi AWS Config API: • DeleteResourceConfig • PutResourceConfig	20 November 2019

Perubahan	Deskripsi	Tanggal Rilis
Paket kesesuaian	Dengan rilis ini, AWS Config memperkenalkan paket kesesuaian. Paket kesesuaian memungkinkan Anda untuk mengemas kumpulan AWS Config aturan dan tindakan remediasi yang kemudian dapat digunakan bersama sebagai satu entitas di seluruh Organisasi. AWS Untuk informasi selengkapnya, lihat Conformance Packs. Untuk informasi selengkapnya APIs, lihat Referensi AWS Config API: • DeleteOrganizationConformancePack • DeleteOrganizationConformancePack • DescribeConformancePacks • DescribeConformancePacks • DescribeConformancePackStatus • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePackStatuses • GetConformancePackComplianceDetails • GetConformancePackComplianceSummary • GetOrganizationConformancePackDetailedStatus, • PutConformancePack • PutOrganizationConformancePack	19 November 2019

Perubahan	Deskripsi	Tanggal Rilis
AWS Config mendukung OpenSearch Layanan Amazon dan jenis AWS Key Management Service sumber daya	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke domain dan AWS Key Management Service kunci OpenSearch Layanan Amazon Anda. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.	11 November 2019
AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • dms-replication-not-public • emr-kerberos-enabled • internet-gateway-authorized-vpc-hanya • kms-cmk-not-scheduled-untuk-penghapusan • sagemaker-notebook-no-direct-akses internet • sagemaker-notebook-instance-kms-kunci-dikonfigurasi • shield-drt-access Untuk informasi selengkapnya, lihat Daftar Aturan AWS Config Terkelola.	10 Oktober 2019

Perubahan	Deskripsi	Tanggal Rilis
AWS Config mendukung jenis sumber daya Amazon RDS	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke Amazon Relational Database Service (Amazon RDS DBCluster) DBCluster dan Snapshot. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.	17 September 2019
AWS Config mendukung jenis sumber daya Amazon QLDB	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke jenis sumber daya buku besar Amazon Quantum Ledger Database (QLDB). Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.	10 September 2019

Perubahan	Deskripsi	Tanggal Rilis
AWS Config memungkinkan Anda menerapkan remediasi otomatis pada sumber daya yang tidak sesuai sebagaimana dievaluasi oleh Aturan AWS Config	Dengan rilis ini, AWS Config memperkenalkan dukungan untuk menerapkan remediasi otomatis menggunakan dokumen AWS Systems Manager otomatisasi pada sumber daya yang tidak sesuai sebagaimana dievaluasi oleh Aturan. AWS Config Untuk informasi selengkapnya, lihat Memulihkan Sumber Daya yang Tidak Sesuai dengan AWS Config. Dengan rilis ini, AWS Config tambahkan yang baru berikut APIs. Untuk informasi selengkapnya, lihat Referensi AWS Config API: • PutRemediationExceptions • DescribeRemediationExceptions • DeleteRemediationExceptions	Selasa, 05 September 2019

Perubahan	Deskripsi	Tanggal Rilis
AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config mendukung aturan terkelola berikut: • alb-http-to-https-pemeriksaan-pengalihan • api-gw-cache-enabled-dan-di enkripsi • api-gw-endpoint-type-periksa • cloudtrail-s3-dataevents-diaktifkan • cloudwatch-log-group-encrypted • ebs-snapshot-public-restorable-periksa • elb-deletion-protection-enabled • lambda-concurrency-check • lambda-dlq-check • lambda-inside-vpc • shield-advanced-enabled-aut orenew • vpc-vpn-2-terowongan Untuk informasi selengkapnya, lihat Daftar Aturan AWS Config Terkelola.	22 Agustus 2019

Perubahan	Deskripsi	Tanggal Rilis
AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config memperbarui aturan terkelola berikut: • cloudfront-viewer-policy-https • ec2- instance-no-public-ip • ec2- -eni security-group-attached-to • efs-encrypted-check • elasticsearch-encrypted-at-rest • elasticsearch-in-vpc-only • redshift-cluster-public-access-periksa • vpc-sg-open-only-to-authorized-ports Untuk informasi selengkapnya, lihat Daftar Aturan AWS Config Terkelola.	31 Juli 2019
AWS Config mendukung jenis EC2 sumber daya Amazon	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigura si ke EC2 sumber daya Amazon berikut; VPCEndpoint, VPCEndpoint Layanan, dan VPCPeering Koneksi. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.	12 Juli 2019

Perubahan	Deskripsi	Tanggal Rilis
AWS Config memungkinkan Anda untuk mengelola AWS Config aturan di semua Akun AWS dalam organisasi	Dengan rilis ini, AWS Config memperkenalkan dukungan untuk mengelola AWS Config aturan di semua Akun AWS dalam organisasi. Anda dapat membuat, memperbarui, dan menghapus AWS Config aturan secara terpusat di semua akun di organisasi Anda. Untuk informasi selengkapnya, lihat Mengelola AWS Config Aturan di Semua Akun di Organisasi Anda. Untuk informasi selengkapnya APIs, lihat Referensi AWS Config API: • PutOrganizationConfigRule • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStatuses • DeleteOrganizationConfigRule	9 Juli 2019
AWS Config mendukung jenis sumber daya Amazon S3 dan Amazon EC2	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke sumber daya Amazon S3 dan AccountPublicAccessBlock sumber EC2 daya Amazon berikut; NatGateway, EgressOnlyInternetGateway, dan. FlowLog Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.	17 Mei 2019

Perubahan	Deskripsi	Tanggal Rilis
AWS Config memperbarui aturan terkelola	Dengan rilis ini, AWS Config memperbarui aturan terkelola berikut: • s3- bucket-public-read-prohibited • s3- bucket-public-write-prohibited Untuk informasi selengkapnya, lihat Daftar Aturan AWS Config Terkelola.	7 Mei 2019
AWS Config memungkinkan Anda untuk menghapus tindakan remediasi menggunakan AWS Management Console.	Dengan rilis ini, AWS Config memperkenalkan dukungan untuk menghapus tindakan remediasi menggunakan. AWS Management Console Untuk informasi selengkapnya, lihat Memulihkan Sumber Daya yang Tidak Sesuai dengan AWS Config.	24 April 2019
AWS Config mendukung aturan terkelola baru	Rilis ini mendukung aturan terkelola baru:fms-shield-resource-policy-periksa. Untuk informasi selengkapnya, lihat Daftar Aturan AWS Config Terkelola.	April 7, 2019

Perubahan	Deskripsi	Tanggal Rilis
AWS Config mendukung jenis sumber daya Amazon API Gateway	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke resource Amazon API Gateway berikut; Api (WebSocket API), RestApi (REST API), Stage (WebSocket API stage), dan Stage (REST API stage). Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.	20 Maret 2019
AWS Config memungkinkan Anda menjalankan kueri tingkat lanjut	Dengan rilis ini, AWS Config menambahkan dukungan untuk menjalankan kueri lanjutan berdasarkan properti konfigurasi sumber daya. Untuk informasi selengkapnya, lihat Menanyakan Status Konfigurasi AWS Sumber Daya Saat Ini dengan AWS Config. Dengan rilis ini, AWS Config tambahkan `SelectResourceConfig` API. Untuk informasi selengkapnya, lihat SelectResourceConfigdi Referensi AWS Config API:	19 Maret 2019

Perubahan	Deskripsi	Tanggal Rilis
AWS Config memungkinkan Anda untuk menetapkan tag sumber daya Anda AWS Config	Dengan rilis ini, AWS Config memperkenalkan dukungan untuk kontrol akses berbasis tag untuk tiga AWS Config sumber daya— `ConfigRule`, `ConfigurationAggregator`, dan`AggregationAuthorization` . Untuk informasi selengkapnya, lihat Menandai Sumber Daya Anda AWS Config. Dengan rilis ini, Anda dapat menambahkan, menghapus, atau mencantumkan tag dari AWS Config sumber daya Anda menggunakan tipe data berikut. Untuk informasi selengkapnya, lihat Referensi AWS Config API: • ListTagsForResource • TagResource • UntagResource	14 Maret 2019

Perubahan	Deskripsi	Tanggal Rilis
AWS Config memungkinkan Anda untuk menerapkan remediasi pada sumber daya yang tidak patuh sebagaimana dievaluasi oleh Aturan AWS Config	Dengan rilis ini, AWS Config memperkenalkan dukungan untuk menerapkan remediasi menggunakan dokumen AWS Systems Manager otomatisasi pada sumber daya yang tidak sesuai sebagaimana dievaluasi oleh Aturan. AWS Config Untuk informasi selengkapnya, lihat Memulihkan Sumber Daya yang Tidak Sesuai dengan AWS Config. Dengan rilis ini, AWS Config tambahkan yang baru berikut APIs. Untuk informasi selengkapnya, lihat Referensi AWS Config API: • DeleteRemediationConfiguration • DescribeRemediationConfigurations • DescribeRemediationExecutionStatus • PutRemediationConfigurations • StartRemediationExecution	12 Maret 2019

Perubahan	Deskripsi	Tanggal Rilis
AWS Config mendukung AWS Config Aturan di Wilayah Tiongkok (Ningxia)	Rilis ini hanya mendukung 54 AWS Config Aturan di Wilayah Tiongkok (Ningxia). Untuk informasi selengkap nya, lihat Daftar Aturan AWS Config Terkelola. Namun, saat ini AWS Config tidak mendukung aturan berikut di Wilayah Tiongkok (Ningxia): • acm-certificate-expiration-check • cmk-backing-key-rotation-di aktifkan • cloudformation-stack-drift-detection -periksa • cloudformation-stack-notification-check • cloud-trail-encryption-enabled • cloud-trail-log-file-validasi-diakti fkan • codebuild-project-envvar-awscred-periksa • codebuild-project-source-repo-url-periksa • codepipeline-deployment-count-check • codepipeline-region-fanout-check • dynamodb-table-encryption-e nabled • elb-acm-certificate-required • volume terenkripsi	12 Maret 2019

Perubahan	Deskripsi	Tanggal Rilis
	• fms-webacl-resource-policy-periksa • fms-webacl-rulegroup-association-periksa • guardduty-enabled-centralized • lambda-function-public-access-dilarang • lambda-function-settings-check • rds-storage-encrypted • root-account-mfa-hardware-mfa-diaktifkan • root-account-mfa-enabled • s3- bucket-blacklisted-actions-prohibited • s3- bucket-policy-grantee-check • s3- bucket-policy-not-more -permisif • s3- bucket-public-read-prohibited • s3- bucket-public-write-prohibited • s3- -diaktifkan bucket-server-side-encryption • s3- bucket-ssl-requests-only	
AWS Config mendukung aturan terkelola baru	Rilis ini mendukung aturan terkelola baru berikut: • iam-user-mfa-enabled • s3- bucket-policy-grantee-check Untuk informasi selengkapnya, lihat Daftar Aturan AWS Config Terkelola.	21 Januari 2019

Perubahan	Deskripsi	Tanggal Rilis
AWS Config mendukung jenis sumber daya Service Catalog	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke sumber daya Service Catalog berikut; CloudFromation produk, produk yang disediakan, dan portofolio. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.	11 Januari 2019
Dukungan aturan terkait layanan AWS Config	Dengan rilis ini, AWS Config tambahkan aturan konfigurasi terkelola baru yang mendukung AWS layanan lain untuk membuat AWS Config Aturan di akun Anda. Untuk informasi selengkapnya, lihat Aturan Terkait Layanan AWS Config.	20 November 2018

Perubahan	Deskripsi	Tanggal Rilis
AWS Config memungkinkan Anda untuk mengumpulkan data konfigurasi sumber daya AWS	Dengan rilis ini, AWS Config memperkenalkan dukungan untuk menggabungkan data konfigurasi sumber daya. AWS Untuk informasi selengkapnya, lihat Melihat Data Kepatuhan dan Inventaris di Dasbor Agregator untuk AWS Config. Dengan rilis ini, AWS Config tambahkan yang baru berikut APIs. Untuk informasi selengkapnya, lihat Referensi AWS Config API: • BatchGetAggregateResourceConfig • GetAggregateDiscoveredResourceCounts • GetAggregateResourceConfig • ListAggregateDiscoveredResources	19 November 2018
AWS Config mendukung aturan terkelola baru	Rilis ini mendukung aturan terkelola baru berikut: • cloudformation-stack-drift-detection-periksa • codepipeline-deployment-count-check • codepipeline-region-fanout-check Untuk informasi selengkapnya, lihat Daftar Aturan AWS Config Terkelola.	19 November 2018

Perubahan	Deskripsi	Tanggal Rilis
AWS Config mendukung aturan terkelola baru	Rilis ini mendukung aturan terkelola baru berikut: • access-keys-rotated • cloud-trail-cloud-watch-logs-diaktifkan • cloud-trail-encryption-enabled • cloud-trail-log-file-validasi-diaktifkan • cmk-backing-key-rotation-diaktifkan • iam-policy-no-statements-with-admin-access • iam-role-managed-policy-periksa • iam-root-access-key-periksa • iam-user-unused-credentials-periksa • mfa-enabled-for-iam-akses konsol • multi-region-cloudtrail-enabled • root-account-hardware-mfa-diaktifkan • vpc-flow-logs-enabled Untuk informasi selengkapnya, lihat Daftar Aturan AWS Config Terkelola.	12 November 2018

Perubahan	Deskripsi	Tanggal Rilis
AWS Config mendukung aturan terkelola baru	Rilis ini mendukung aturan terkelola baru berikut: • dynamodb-table-encryption-enabled • elb-logging-enabled • rds-instance-public-access-periksa • vpc-default-security-group-tertutup Untuk informasi selengkapnya, lihat Daftar Aturan AWS Config Terkelola.	24 Oktober 2018
Dukungan riwayat kepatuhan	Dengan rilis ini, AWS Config sekarang mendukung penyimpanan riwayat kepatuhan sumber daya seperti yang dievaluasi oleh AWS Config Aturan. Untuk informasi selengkapnya, lihat Melihat Garis Waktu Riwayat Kepatuhan untuk Sumber Daya dan Aturan.	18 Oktober 2018
Dukungan Wilayah Agregasi Data multi-wilayah multi-akun	Dengan rilis ini, Agregasi Data multi-wilayah multi-akun sekarang didukung di enam Wilayah baru. Untuk informasi selengkapnya, lihat Multi-Account Multi-Region Data Aggregation.	4 Oktober 2018

Perubahan	Deskripsi	Tanggal Rilis
AWS Config mendukung izin tingkat sumber daya untuk tindakan Aturan AWS Config APIs	Dengan rilis ini, AWS Config mendukung izin tingkat sumber daya untuk tindakan API Aturan tertentu. AWS Config Untuk informasi selengkapnya tentang dukungan APIs, lihatIzin Tingkat Sumber Daya yang Didukung untuk Tindakan API Aturan AWS Config.	1 Oktober 2018
AWS Config mendukung jenis CodePipeline sumber daya	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke jenis AWS CodePipeline sumber daya. Untuk informasi selengkap nya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.	September 12, 2018

Perubahan	Deskripsi	Tanggal Rilis
AWS Config mendukung aturan terkelola baru	Rilis ini mendukung aturan terkelola baru berikut: • ec2- -manajer instance-managed-by-systems • ec2- -periksa managedinstance-association-compliance-status • ec2- -periksa managedinstance-patch-compliance-status • guardduty-enabled-centralized • rds-snapshots-public-prohibited • s3- bucket-blacklisted-actions-prohibited • s3- bucket-policy-not-more -permisif Untuk informasi selengkapnya, lihat Daftar Aturan AWS Config Terkelola.	5 September 2018
AWS Config mendukung jenis sumber daya AWS Systems Manager	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi pada kepatuhan patch AWS Systems Manager dan jenis sumber daya kepatuhan asosiasi. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.	9 Agustus 2018

Perubahan	Deskripsi	Tanggal Rilis
AWS Config memungkinkan Anda untuk menghapus AWS Config data Anda menggunakan AWS Management Console	Dengan rilis ini, AWS Config memperkenalkan dukungan untuk penggunaan AWS Management Console periode retensi. Di dalam AWS Management Console, Anda dapat memilih periode penyimpanan data kustom untuk Anda`ConfigurationItems`. Untuk informasi selengkapnya, lihat Menghapus Data AWS Config.	7 Agustus 2018
AWS Config mendukung jenis AWS Shield sumber daya	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke jenis sumber daya AWS Shield Perlindungan. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.	7 Agustus 2018
AWS Config mendukung AWS PrivateLink	Dengan rilis ini, AWS Config mendukung AWS PrivateLink, memungkinkan Anda untuk merutekan data antara Amazon Virtual Private Cloud (VPC) dan AWS Config seluruhnya di dalam jaringan. AWS Untuk informasi selengkapnya, lihat Menggunakan AWS Config dengan Antarmuka Amazon VPC Endpoints.	31 Juli 2018

Perubahan	Deskripsi	Tanggal Rilis
AWS Config memungkinkan Anda untuk menghapus AWS Config data Anda	Dengan rilis ini, AWS Config memperkenalkan dukungan untuk periode retensi. AWS Config memungkinkan Anda untuk menghapus data Anda dengan menentukan periode retensi untuk Anda`ConfigurationItems` . Untuk informasi selengkapnya, lihat Menghapus Data AWS Config. Dengan rilis ini, AWS Config tambahkan yang baru berikut APIs. Untuk informasi selengkapnya, lihat Referensi AWS Config API: • PutRetentionConfiguration • DescribeRetentionConfigurations • DeleteRetentionConfiguration	25 Mei 2018
AWS Config mendukung aturan terkelola baru	Rilis ini mendukung dua aturan terkelola baru berikut: • lambda-function-settings-check • s3- bucket-replication-enabled • iam-policy-blacklisted-check Untuk informasi selengkapnya, lihat Daftar Aturan AWS Config Terkelola.	10 Mei 2018

Perubahan	Deskripsi	Tanggal Rilis
AWS Config mendukung jenis AWS X-Ray sumber daya	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke jenis AWS X-Ray EncryptionConfig sumber daya. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.	1 Mei 2018
AWS Config mendukung jenis AWS Lambda sumber daya dan satu aturan terkelola baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke jenis sumber daya AWS Lambda fungsi. Untuk informasi selengkap nya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config. Rilis ini juga mendukung aturan lambda-function-public-access-dilarang terkelola. Untuk informasi selengkapnya, lihat AWS Config Aturan yang Dikelola.	25 April 2018
AWS Config mendukung jenis AWS Elastic Beanstalk sumber daya	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi pada sumber daya AWS Elastic Beanstalk Aplikasi, Versi Aplikasi, dan Lingkungan. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.	April 24, 2018

Perubahan	Deskripsi	Tanggal Rilis
AWS Config mendukung aturan terkelola baru	Rilis ini mendukung dua aturan terkelola baru berikut: • fms-webacl-resource-policy-periksa • fms-webacl-rulegroup-association-periksa Untuk informasi selengkapnya, lihat Daftar Aturan AWS Config Terkelola.	4 April 2018

Perubahan	Deskripsi	Tanggal Rilis
Agregasi data multi-wilayah multi-akun	Dengan rilis ini, AWS Config memperkenalkan agregasi data multi-wilayah multi-akun. Fitur ini memungkinkan Anda untuk mengumpulkan AWS Config data dari beberapa akun atau organisasi dan beberapa wilayah ke dalam akun agregator. Untuk informasi selengkap nya, lihat Multi-Account Multi-Region Data Aggregation. Dengan rilis ini, AWS Config tambahkan yang baru berikut APIs. Untuk informasi selengkapnya, lihat Referensi AWS Config API: • PutConfigurationAggregator • DescribePendingAggregationRequests • DeletePendingAggregationRequest • PutAggregationAuthorization • DescribeAggregationAuthorizations • GetAggregateConfigRuleComplianceSummary • DescribeAggregateComplianceByConfigRules • GetAggregateComplianceDetailsByConfigRule • DescribeConfigurationAggregators • DescribeConfigurationAggregatorSourcesStatus • DeleteAggregationAuthorization • DeleteConfigurationAggregator	4 April 2018

Perubahan	Deskripsi	Tanggal Rilis
Pemantauan AWS Config dengan CloudWatch Acara Amazon	Dengan rilis ini, gunakan Amazon CloudWatch Events untuk mendeteksi dan bereaksi terhadap perubahan status AWS Config peristiwa. Untuk informasi selengkapnya, lihat Pemantauan AWS Config dengan Amazon EventBridge.	29 Maret 2018
Operasi API baru	Dengan rilis ini, AWS Config tambahkan dukungan untuk BatchGetResourceConfigAPI, memungkinkan Anda untuk mengambil status saat ini dari satu atau beberapa sumber daya Anda.	20 Maret 2018
AWS Config mendukung jenis AWS WAF RuleGroup sumber daya	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi pada sumber daya AWS WAF RuleGroup dan AWS WAF RuleGroup Regional. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.	15 Februari 2018

Perubahan	Deskripsi	Tanggal Rilis
AWS Config mendukung aturan terkelola baru	Rilis ini mendukung aturan terkelola baru berikut: • elb-acm-certificate-required • elb-custom-security-policy-ssl-periksa • elb-predefined-security-policy-ssl-periksa • codebuild-project-envvar-awscred-periksa • codebuild-project-source-repo-url-periksa • iam-group-has-users-periksa • s3- -diaktifkan bucket-server-side-encryption Untuk informasi selengkapnya, lihat Daftar Aturan AWS Config Terkelola.	25 Januari 2018
AWS Config mendukung jenis sumber daya Elastic Load Balancing	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi pada penyeimbang beban klasik Elastic Load Balancing. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.	17 November 2017

Perubahan	Deskripsi	Tanggal Rilis
AWS Config mendukung Amazon CloudFront dan jenis AWS WAF sumber daya	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigura si pada CloudFront distribusi dan distribusi streaming Anda. Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke sumber daya berikut AWS WAF dan AWS WAF Regional; aturan, aturan, dan Web ACL berdasarkan tingkat. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.	15 November 2017
AWS Config mendukung jenis AWS CodeBuild sumber daya	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi pada AWS CodeBuild proyek Anda. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.	20 Oktober 2017

Perubahan	Deskripsi	Tanggal Rilis
AWS Config mendukung sumber daya Auto Scaling dan satu aturan terkelola baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigura si ke sumber daya Auto Scaling berikut; grup, konfigurasi peluncura n, tindakan terjadwal, dan kebijakan penskalaan. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config. Rilis ini juga mendukung aturan terkelola berikut: • autoscaling-group-elb-healthcheck-diperlukan Untuk informasi selengkapnya, lihat AWS Config Aturan yang Dikelola.	18 September 2017
AWS Config mendukung jenis AWS CodeBuild sumber daya	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi pada AWS CodeBuild proyek Anda. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.	20 Oktober 2017

Perubahan	Deskripsi	Tanggal Rilis
AWS Config mendukung sumber daya Auto Scaling dan satu aturan terkelola baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigura si ke sumber daya Auto Scaling berikut; grup, konfigurasi peluncura n, tindakan terjadwal, dan kebijakan penskalaan. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config. Rilis ini juga mendukung aturan terkelola berikut: • autoscaling-group-elb-healthcheck-diperlukan Untuk informasi selengkapnya, lihat AWS Config Aturan yang Dikelola.	18 September 2017

Perubahan	Deskripsi	Tanggal Rilis
AWS Config mendukung tipe sumber daya tabel DynamoDB dan satu aturan terkelola baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke tabel DynamoDB Anda. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config. Rilis ini mendukung aturan terkelola berikut: • dynamodb-autoscaling-enabled Untuk informasi selengkapnya, lihat AWS Config Aturan yang Dikelola.	8 September 2017
AWS Config mendukung dua aturan terkelola baru untuk Amazon S3	Rilis ini mendukung dua aturan terkelola baru: • s3- bucket-public-read-prohibited • s3- bucket-public-write-prohibited Untuk informasi selengkapnya, lihat AWS Config Aturan yang Dikelola.	14 Agustus 2017

Perubahan	Deskripsi	Tanggal Rilis
Halaman baru di AWS Config konsol	Anda dapat menggunakan Dasbor di AWS Config konsol untuk melihat hal berikut: • Jumlah total sumber daya • Jumlah total aturan • Jumlah sumber daya yang tidak patuh • Jumlah aturan yang tidak patuh Untuk informasi selengkapnya, lihat Melihat AWS Config Dasbor.	17 Juli 2017
Operasi API baru	Anda dapat menggunakan GetDiscoveredResourceCountsoperasi untuk mengembalikan jumlah jenis sumber daya, jumlah setiap jenis sumber daya, dan jumlah total sumber daya AWS Config yang direkam di Wilayah untuk Anda Akun AWS.	17 Juli 2017

Perubahan	Deskripsi	Tanggal Rilis
AWS Config mendukung jenis sumber daya AWS CloudFormation tumpukan dan satu aturan terkelola baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi pada AWS CloudFormation tumpukan Anda. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config. Rilis ini mendukung aturan terkelola berikut: • cloudformation-stack-notification-check Untuk informasi selengkapnya, lihat AWS Config Aturan yang Dikelola.	6 Juli 2017
Konten baru dan diperbarui	Rilis ini menambahkan dukungan untuk AWS Config Aturan di Wilayah Kanada (Tengah) dan Wilayah Amerika Selatan (São Paulo). Untuk semua wilayah yang mendukung AWS Config dan Aturan Konfigurasi, lihat Wilayah AWS dan Titik Akhir di. Referensi Umum AWS	5 Juli 2017

Perubahan	Deskripsi	Tanggal Rilis
Konten baru dan diperbarui	AWS Config Aturan tersedia di AWS GovCloud (US) Wilayah. Untuk informasi selengkapnya, silakan lihat Panduan Pengguna AWS GovCloud (US). Untuk wilayah yang mendukung AWS Config, lihat Wilayah AWS dan Titik Akhir di. Referensi Umum AWS	8 Juni 2017
AWS Config mendukung jenis sumber daya CloudWatch alarm Amazon dan tiga aturan terkelola baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi pada CloudWatch alarm Amazon Anda. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config. Rilis ini mendukung tiga aturan terkelola baru: • cloudwatch-alarm-action-check • cloudwatch-alarm-resource-check • cloudwatch-alarm-settings-check Untuk informasi selengkapnya, lihat AWS Config Aturan yang Dikelola.	1 Juni 2017

Perubahan	Deskripsi	Tanggal Rilis
Konten baru dan diperbarui	Rilis ini mendukung penetapan nomor versi aplikasi untuk aturan terkelola berikut: • ec2- managedinstance-applications-blacklisted • ec2- managedinstance-applications-required Untuk informasi selengkapnya, lihat AWS Config Aturan yang Dikelola.	1 Juni 2017
Konten baru dan diperbarui	Rilis ini menambahkan dukungan untuk AWS Config Rules in the Asia Pacific (Mumbai) Region. Untuk informasi lebih lanjut, lihat Wilayah AWS dan Titik Akhir di. Referensi Umum AWS	April 27, 2017

Perubahan	Deskripsi	Tanggal Rilis
Konten baru dan diperbarui	Rilis ini mendukung pengalaman konsol yang diperbarui untuk menambahkan aturan AWS Config terkelola ke akun Anda untuk pertama kalinya. Saat menyiapkan AWS Config Aturan untuk pertama kalinya atau di Wilayah baru, Anda dapat mencari aturan AWS terkelola berdasarkan nama, deskripsi, atau label. Anda dapat memilih Pilih semua untuk memilih semua aturan atau memilih Hapus semua untuk menghapus semua aturan. Untuk selengkapnya, lihat Menambahkan, Melihat, Memperbarui, dan Menghapus Aturan (Konsol).	5 April 2017

Perubahan	Deskripsi	Tanggal Rilis
AWS Config mendukung aturan terkelola baru	Rilis ini mendukung aturan terkelola baru berikut: • acm-certificate-expiration-check • ec2- instance-detailed-monitoring-enabled • ec2- managedinstance-inventory-blacklisted • ec2- volume-inuse-check • iam-user-group-membership-periksa • iam-user-no-policies-periksa • s3- bucket-ssl-requests-only Untuk informasi selengkapnya, lihat Daftar Aturan AWS Config Terkelola.	21 Februari 2017
Konten baru dan diperbarui	Rilis ini menambahkan dukungan untuk AWS Config Aturan di Wilayah Eropa (London). Untuk informasi lebih lanjut, lihat Wilayah AWS dan Titik Akhir di. Referensi Umum AWS	21 Februari 2017
Konten baru dan diperbarui	Rilis ini menambahkan AWS CloudFormation template untuk aturan AWS Config terkelola. Anda dapat menggunakan templat untuk membuat aturan terkelola untuk akun Anda. Untuk informasi selengkapnya, lihat Membuat Aturan AWS Config Terkelola Dengan AWS CloudFormation Template.	Februari 16, 2017

Perubahan	Deskripsi	Tanggal Rilis
Konten baru dan diperbarui	Rilis ini menambahkan dukungan untuk mode pengujian baru untuk `PutEvaluations` API. Setel `TestMode` parameter ke true dalam aturan kustom Anda untuk memverifikasi apakah AWS Lambda fungsi Anda akan memberikan hasil evaluasi AWS Config. Tidak ada pembaruan yang terjadi pada evaluasi Anda yang ada, dan hasil evaluasi tidak dikirim ke AWS Config. Untuk informasi selengkapnya, lihat PutEvaluations di dalam Referensi API AWS Config .	Februari 16, 2017
Konten baru dan diperbarui	Rilis ini menambahkan dukungan untuk AWS Config Rules in the Asia Pacific (Seoul), dan US West (N. California) Regions. Untuk informasi lebih lanjut, lihat Wilayah AWS dan Titik Akhir di. Referensi Umum AWS	Desember 21, 2016
Konten baru dan diperbarui	Rilis ini menambah dukungan untuk AWS Config di Wilayah Eropa (London). Untuk informasi lebih lanjut, lihat Wilayah AWS dan Titik Akhir di. Referensi Umum AWS	13 Desember 2016
Konten baru dan diperbarui	Rilis ini menambahkan dukungan untuk AWS Config di Wilayah Kanada (Tengah). Untuk informasi lebih lanjut, lihat Wilayah AWS dan Titik Akhir di. Referensi Umum AWS	8 Desember 2016

Perubahan	Deskripsi	Tanggal Rilis
AWS Config mendukung jenis sumber daya Amazon Redshift dan dua aturan terkelola baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi pada klaster Amazon Redshift, grup parameter cluster, grup keamanan klaster, snapshot klaster, grup subnet klaster, dan langganan acara. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config. Rilis ini mendukung dua aturan terkelola baru: • redshift-cluster-configuration-check • redshift-cluster-maintenancesettings-check Untuk informasi selengkapnya, lihat Daftar Aturan AWS Config Terkelola.	Desember 7, 2016
Konten baru dan diperbarui	Rilis ini menambahkan dukungan untuk aturan terkelola baru: • dynamodb-throughput-limit-check Untuk informasi selengkapnya, lihat Daftar Aturan AWS Config Terkelola.	Desember 7, 2016
Konten baru dan diperbarui	Rilis ini menambahkan dukungan untuk membuat hingga 50 aturan per Wilayah di akun. Untuk informasi selengkapnya, lihat Batas AWS Konfigurasi di. Referensi Umum AWS	Desember 7, 2016

Perubahan	Deskripsi	Tanggal Rilis
AWS Config mendukung jenis sumber daya inventaris instans terkelola untuk Amazon EC2 Systems Manager dan tiga aturan terkelola baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigura si perangkat lunak pada instans terkelola dengan dukungan untuk inventaris instans terkelola. Untuk informasi selengkapnya, lihat Recording Software Configuration for Managed Instances. Rilis ini mendukung tiga aturan terkelola baru: • ec2- managedinstance-inventory-b lacklisted • ec2- managedinstance-application s-required • ec2- managedinstance-platform-ch eck Untuk informasi selengkapnya, lihat Daftar Aturan AWS Config Terkelola.	1 Desember 2016
Konten baru dan diperbarui	AWS Config tersedia di Wilayah Tiongkok (Beijing).	24 Oktober 2016

Perubahan	Deskripsi	Tanggal Rilis
AWS Config mendukung sumber daya bucket Amazon S3 dan dua aturan terkelola baru	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke bucket Amazon S3 Anda. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config. Rilis ini mendukung dua aturan terkelola baru: • s3- bucket-logging-enabled • s3- bucket-versioning-enabled Untuk informasi selengkapnya, lihat AWS Config Aturan yang Dikelola.	18 Oktober 2016
Konten baru dan diperbarui	Rilis ini menambahkan dukungan untuk AWS Config dan AWS Config Aturan di Wilayah Timur AS (Ohio). Untuk informasi lebih lanjut, lihat Wilayah AWS dan Titik Akhir di. Referensi Umum AWS	17 Oktober 2016

Perubahan	Deskripsi	Tanggal Rilis
Aturan terkelola baru dan diperbarui	Pembaruan ini menambahkan dukungan untuk delapan aturan terkelola baru: • approved-amis-by-id • approved-amis-by-tag • db-instance-backup-enabled • desired-instance-type • ebs-optimized-instance • iam-password-policy • rds-multi-az-support • rds-storage-encrypted Anda dapat menentukan beberapa nilai parameter untuk aturan berikut: • desired-instance-tenancy • tag yang dibutuhkan Untuk informasi selengkapnya, lihat Daftar Aturan AWS Config Terkelola.	Oktober 4, 2016

Perubahan	Deskripsi	Tanggal Rilis
Konten baru dan diperbarui untuk AWS Config konsol	Pembaruan ini menambahkan dukungan untuk melihat aktivitas AWS CloudTrail API di AWS Config timeline. Jika CloudTrai l masuk ke akun Anda, Anda dapat melihat peristiwa membuat, memperbarui, dan menghapus API untuk perubahan konfigurasi pada sumber daya Anda. Untuk informasi selengkapnya, lihat Melihat Riwayat Kepatuhan untuk AWS Sumber Daya Anda dengan AWS Config.	September 06, 2016
AWS Config mendukung jenis sumber daya Elastic Load Balancing	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi pada penyeimbang beban aplikasi Elastic Load Balancing Anda. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.	31 Agustus 2016
Konten baru dan diperbarui	Rilis ini menambahkan dukungan untuk AWS Config Rules in the Asia Pacific (Singapura), dan Asia Pacific (Sydney) Regions. Untuk informasi lebih lanjut, lihat Wilayah AWS dan Titik Akhir di. Referensi Umum AWS	18 Agustus 2016

Perubahan	Deskripsi	Tanggal Rilis
Konten baru dan diperbarui untuk AWS Config Aturan	Pembaruan ini menambahkan dukungan untuk membuat aturan yang dapat dipicu oleh perubahan konfigurasi dan pada frekuensi periodik yang Anda pilih. Untuk informasi selengkapnya, lihat Komponen AWS Config Aturan. Pembaruan ini juga menambahk an dukungan untuk mengevalu asi sumber daya Anda secara manual terhadap aturan Anda dan menghapus hasil evaluasi. Untuk informasi selengkapnya, lihat Mengevaluasi Sumber Daya Anda dengan Aturan AWS Config. Pembaruan ini juga menambahkan dukungan untuk mengevaluasi jenis sumber daya tambahan menggunak an aturan khusus.	25 Juli 2016

Perubahan	Deskripsi	Tanggal Rilis
AWS Config mendukung jenis sumber daya Amazon RDS dan AWS Certificate Manager (ACM)	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke instans DB Amazon Relational Database Service (Amazon RDS), grup keamanan DB, snapshot DB, grup subnet DB, dan langganan acara. Anda juga dapat menggunak an AWS Config untuk merekam perubahan konfigurasi pada sertifikat yang disediakan oleh ACM. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.	21 Juli 2016
Informasi terbaru tentang mengelola perekam konfigurasi	Pembaruan ini menambahkan langkah-langkah untuk mengganti nama dan menghapus perekam konfigurasi ke. Bekerja dengan perekam konfigurasi	Juli 07, 2016
Pembuatan peran yang disederhanakan dan kebijakan yang diperbarui	Dengan pembaruan ini, membuat peran IAM untuk AWS Config disederhanakan. Peningkatan ini tersedia di wilayah yang mendukung aturan Config. Untuk mendukung peningkatan ini, langkah-langkah di Menyiapkan AWS Config dengan Konsol diperbarui, kebijakan contoh di Izin untuk Bucket Amazon S3 untuk AWS Config Saluran Pengirima n diperbarui, dan kebijakan contoh di Contoh kebijakan berbasis identitas untuk AWS Config diperbarui.	31 Maret 2016

Perubahan	Deskripsi	Tanggal Rilis
Contoh fungsi dan peristiwa untuk aturan Config	Pembaruan ini menyediakan fungsi contoh yang diperbarui.	29 Maret 2016
AWS Config Aturan GitHub repositori	Pembaruan ini menambahkan informasi tentang GitHub repositori AWS Config Aturan ke. Mengevaluasi Sumber Daya dengan Aturan AWS Config Repositori ini menyediakan contoh fungsi untuk aturan kustom yang dikembangkan dan disumbangkan oleh AWS Config pengguna.	1 Maret 2016
AWS Config Aturan	Rilis ini memperkenalkan AWS Config Aturan. Dengan aturan, Anda dapat menggunakan AWS Config untuk mengevaluasi apakah AWS sumber daya Anda sesuai dengan konfigurasi yang Anda inginkan. Untuk informasi selengkapnya, lihat Mengevaluasi Sumber Daya dengan Aturan AWS Config.	18 Desember 2015
AWS Config mendukung jenis sumber daya IAM	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi pada pengguna IAM, grup, peran, dan kebijakan yang dikelola pelanggan. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.	Desember 10, 2015

Perubahan	Deskripsi	Tanggal Rilis
AWS Config mendukung Host EC2 khusus	Dengan rilis ini, Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke host EC2 Khusus Anda. Untuk informasi selengkapnya, lihat Jenis Sumber Daya yang Didukung untuk AWS Config.	November 23, 2015
Informasi izin yang diperbarui	Pemutakhiran ini menambahkan informasi tentang kebijakan AWS terkelola berikut untuk AWS Config: • `AWS_ConfigRole` — Memberikan AWS Config izin untuk mendapatkan detail konfigurasi tentang sumber daya Anda. Untuk informasi selengkapnya, lihat Kebijakan Peran IAM untuk Mendapatkan Detail Konfigurasi. • `AWSConfigUserAccess` — Memberikan akses hanya-baca ke pengguna. AWS Config Untuk informasi selengkapnya, lihat Akses hanya-baca ke AWS Config.	19 Oktober 2015
AWS Config Pratinjau aturan	Rilis ini memperkenalkan pratinjau AWS Config Aturan. Dengan aturan, Anda dapat menggunakan AWS Config untuk mengevaluasi apakah AWS sumber daya Anda sesuai dengan konfigurasi yang Anda inginkan. Untuk informasi selengkapnya, lihat Mengevaluasi Sumber Daya dengan Aturan AWS Config.	7 Oktober 2015

Perubahan	Deskripsi	Tanggal Rilis
Konten baru dan diperbarui	Rilis ini menambahkan kemampuan untuk mencari sumber daya yang AWS Config telah ditemukan. Untuk informasi selengkapnya, lihat Mencari Sumber Daya yang Ditemukan oleh AWS Config.	27 Agustus 2015
Konten baru dan diperbarui	Rilis ini menambahkan kemampuan untuk memilih jenis sumber daya yang AWS Config merekam. Untuk informasi selengkapnya, lihat Merekam AWS Sumber Daya dengan AWS Config.	Juni 23, 2015
Konten baru dan diperbarui	Rilis ini menambahkan dukungan untuk wilayah berikut: Asia Pasifik (Tokyo), Asia Pasifik (Singapura), Eropa (Frankfurt), Amerika Selatan (São Paulo), dan AS Barat (California N.). Untuk informasi lebih lanjut, lihat Wilayah AWS dan Titik Akhir.	April 6, 2015
Panduan baru	Rilis ini memperkenalkan AWS Config.	12 November 2014

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.